PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/08

A1

(11) International Publication Number: **WO 96/26505**

(43) International Publication Date: 29 August 1996 (29.08.96)

(21) International Application Number: PCT/CA96/00104

(22) International Filing Date: 22 February 1996 (22.02.96)

(30) Priority Data:
9503662.0 23 February 1995 (23.02.95) GB

(71) Applicant *(for all designated States except US)*: OMEGA DIGITAL DATA INC. [-/-]; * (**).

(71)(72) Applicant and Inventor *(for US only)*: COVELEY, Michael [US/CA]; 45 Ironshield Crescent, Thronhill, Ontario L3T 3K7 (CA).

(74) Agent: RUSTON, David, A.; Sim & McBurney, Suite 701, 330 University Avenue, Toronto, Ontario M5G 1R7 (CA).

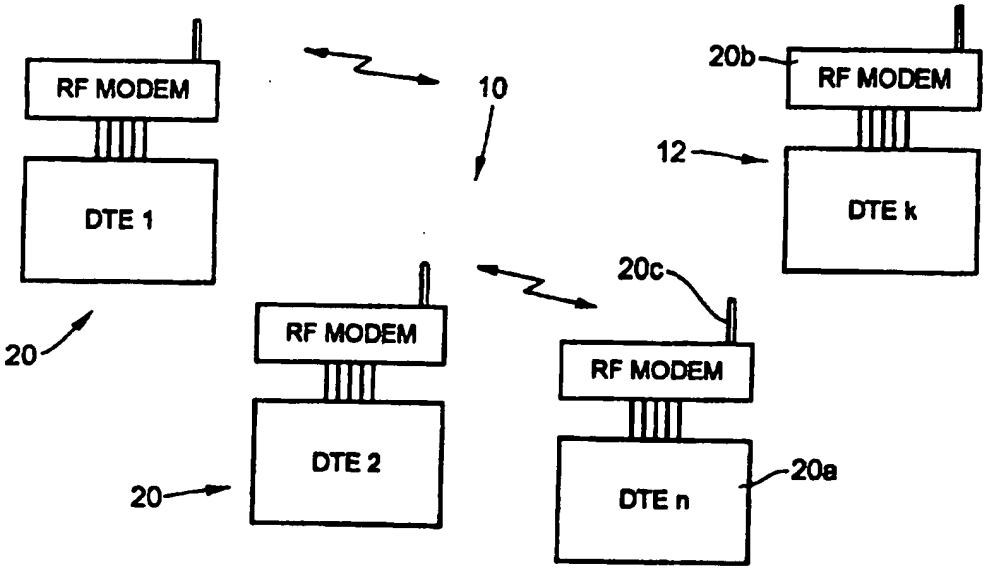
(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: FREE-ROAMING REMOTE HAND-HELD POINT-OF-SALE TERMINAL



(57) Abstract

A financial transaction system (10) is provided in which a user is given a portable RF financial transaction terminal (20) with which to enter transaction data via a keypad (52) or read a UPC bar code on merchandise via a CCD scanner (42) and read their credit, debit or smart card. The RF financial transaction terminal (20) transmits the transaction and card data to a central network controller (12) via a RF communications link. The central network controller (12) in turn conveys the transaction and card data to the host computers at a financial institution where the transaction is processed in real-time. The financial institutions return verification data to the central network controller which is passed back to the RF financial transaction terminal via the RF communications link. The RF financial transaction terminal then generates a printed receipt of the transaction for the user. All of this may be done while the RF financial transaction terminal and the user's credit, debit or smart card remains in the total custody of the user. The user is therefore relieved from having to proceed to an ABM, retail platform, cashier's desk, etc.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Paso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

FREE-ROAMING REMOTE HAND-HELD POINT-OF-SALE TERMINAL

TECHNICAL FIELD

The present invention relates in general to financial transaction recording systems, and more particularly to a portable hand-held financial transaction terminal and to a financial transaction system including a plurality of portable radio frequency (RF) financial transaction terminals operable to establish a radio frequency communications link with a central network controller to transmit financial transaction data thereto.

BACKGROUND ART

Financial transaction devices to read data stored on credit, debit and/or smart cards to complete a financial transaction are known. Existing systems, such as automated banking machines (ABMs) require users to walk to and from an often far-off central retail transaction platform to complete a financial transaction. More recently, debit-card systems have been provided at retail transaction platforms which allow a user to remotely enter his or her personal identification number (PIN) to directly withdraw funds from a financial institution to complete a financial transaction.

Both the ABM and debit-card systems suffer from the disadvantage of requiring the user to proceed to a particular retail transaction platform to complete a financial transaction. Also, these systems require the user to loose custody of their credit or debit card to a sales person, or in the case of ABMs to the machine itself.

It is therefore an object of the present invention to obviate or mitigate at least one of the aforesaid disadvantages.

DISCLOSURE OF THE INVENTION

According to one aspect of the present invention there is provided a portable radio frequency financial transaction terminal comprising:

a housing;

input means to allow transaction data to be entered therein;

a card reader to receive and read credit, debit or smart cards;

a processor in communication with said input means and said card reader to receive and process transaction and card data; and

a radio frequency transmitter to transmit said transaction and card data to a remote site whereat a transaction can be processed.

According to another aspect of the present invention there is provided a financial transaction system comprising:

a plurality of portable radio frequency financial transaction terminals to receive transaction and debit, credit or smart card data; and

a central network controller in communication with each of said portable radio frequency financial transaction terminals via a RF communications link, said central network controller receiving said transaction and card data transmitted by said portable radio frequency financial transaction terminals and conveying said transaction and card data to a financial institution whereat transactions can be processed.

In still yet another aspect of the present invention there is provided a financial transaction terminal comprising:

a housing;

input means to allow transaction data to be entered therein;

a card reader to receive and read credit, debit or smart cards;

a processor in communication with said input means and said card reader to receive and process transaction and card data; and

shock absorbing means acting between said card reader and said housing to inhibit shocks from being applied to said card reader.

In still yet another aspect of the present invention there is provided a financial transaction terminal comprising:

a housing;

input means to allow transaction data to be entered therein;

a card reader to receive and read credit, debit or smart cards;

a processor in communication with said input means and said card reader to receive and process transaction and card data; and

a pistol grip depending from said housing to facilitate carrying of said terminal, said pistol grip being movable between extended and retracted positions.

According to one embodiment of the present invention, a financial transaction system is provided in which the user is given a portable RF financial transaction terminal with which to enter transaction data via a keypad or read a UPC bar code on merchandise via a CCD scanner, read their credit, debit or smart card, and obtain a printed receipt of the transaction. All of this may be done while the RF financial transaction terminal and the user's card remain in the total custody of the user. The user is therefore relieved from having to proceed to an ABM, retail platform, cashier's desk, etc.

Preferably, each RF financial transaction terminal includes a motherboard with a main CPU module controlling four input/output interfaces capable of communicating with a bar code reader, a printer, a card reader interface and a radio frequency transmitter/receiver interface. The main CPU module also communicates with a secure module for providing cryptographic security control via a secure chip which interfaces with an RS-232 interface, a speaker, a display and a keypad. A battery backup is provided along with SRAM and flash memory containing start-up routines and system download routines.

The RF financial transaction terminal is designed for easy use and includes a simple user card insertion device for reading credit, debit and courtesy cards, as well as read/write sensing for smart card applications. The printer consumes low power and is designed for quiet operation and easy loading of paper. The display preferably comprises an LCD screen incorporating a split screen feature for portraying not only encrypted/driven information via prompting, but also predetermined application software for tracking daily sales, adjusting inventories and audit trails, scheduling, daily accruals, etc. The casing for the RF financial transaction terminal is designed to be convertible from an ergonomic pistol grip shape to a palm grip shape.

The present invention provides advantages in that transactions can be carried out at the location of a user without requiring the user to travel to an ABM, retail platform etc. and without requiring the user to give up custody of their card. Also, transactions entered into the RF financial transaction terminals are processed and verified in real-time since the transaction data is forwarded to host computers at a financial institution via a RF communications link and a central network controller

where the transaction data is verified and processed. Confirmation that the transaction has been verified and processed is sent back to the RF financial transaction terminal by the financial institution via the central network controller and RF communications link.

BRIEF DESCRIPTION OF THE DRAWING

Embodiments of the present invention will now be described more fully with reference to the following drawings, in which:

Figure 1a is a block diagram of a portable radio frequency financial transaction terminal for a financial transaction system in accordance with the present invention;

Figure 1b is a block diagram of a secure chip forming part of the portable radio frequency financial transaction terminal of Figure 1a;

Figure 2 is a block diagram of a central network controller for a financial transaction system in accordance with the present invention;

Figure 3a is a schematic representation of the financial transaction system in accordance with the present invention;

Figure 3b is a schematic representation of a communications protocol utilized between the portable radio frequency financial transaction terminals and the central network controller;

Figures 4 and 5 are flow charts illustrating the method by which the communications protocol of Figure 3b is implemented;

Figure 6a is a partly exploded perspective view of the portable radio frequency financial transaction terminal of Figure 1a;

Figures 6b to 6e are perspective views of the components constituting a handle forming part of the portable radio frequency financial transaction terminal of Figure 6a;

Figure 7 are perspective views of the handle of Figures 6b to 6e in various positions;

Figure 8 is an exploded perspective cut-away view of a portion of the portable radio frequency financial transaction terminal of Figure 6a;

Figure 9 is a partly exploded perspective view of an alternative embodiment of a portable radio frequency financial transaction terminal in accordance with the present invention;

Figure 10 is a partial perspective view of the portable radio frequency financial transaction terminal of Figure 6a in combination with a power supply charging dock;

Figure 11 is a partially cut-away perspective view of a charging and carrying nest for the portable radio frequency financial transaction terminal of Figure 6a;

Figures 12a and 12b are exploded top plan and side elevational views, respectively, of components of the portable radio frequency financial transaction terminal of Figure 6a; and

Figure 13 is a partly exploded perspective view of another embodiment of a portable radio frequency financial transaction terminal in accordance with the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Referring now to Figure 3, a financial transaction system is shown and is generally indicated to by reference numeral 10. Financial transaction system 10 includes a central network controller 12 and a plurality of portable hand-held radio frequency (RF) financial transaction terminals 20. In this particular example, the financial transaction system 10 supports up to thirty-two (32) RF financial transaction terminals. The central network controller 12 and the RF financial transaction terminals 20 communicate via a wireless RF communications link. The central network controller 12 also communicates with host computers at financial institutions (not shown) via DATAPAC services or via an ISDN interface as will be described to provide real-time transaction processing with the host computers. Each RF financial transaction terminal 20 includes a financial transaction data module (DTE) 20a for collecting financial transaction data and a RF transceiver, in this particular example a RF modem 20b for transmitting financial transaction data to the central network controller 12 and for receiving transaction verification data from the central network controller 12. The RF modem 20b includes an internal microcontroller unit (MCU) and an antenna 20c.

Financial transactions are carried out by bringing a RF financial transaction terminal 20 to the location of a user. Transaction data is entered into the DTE 20a of the RF financial transaction terminal either via an input keypad or a bar code reader. The user's debit or credit card is read by the RF financial transaction terminal 20 in the presence of the user. The user is required to enter a PIN or password via the input keypad. The RF financial transaction terminal 20 does not display the entered PIN or password data and encrypts the data to inhibit the data from being accessed by unauthorized parties as the data is communicated between the RF financial transaction terminal 20, the central network controller 12 and the host computers. The RF modem 20b of the RF financial transaction terminal 20 transmits the encrypted data to the central network controller 12 which in turn conveys the information to a financial institution so that the transaction can be verified and processed. Once processed, the central network controller 12 transmits verification data received from the host computer to the RF financial transaction terminal 20 to inform the user that the transaction has been verified and processed. The RF team financial transaction terminal in turn prints a receipt confirming that the transaction has been verified and processed. Further details of the financial transaction system 10 will now be described.

RF Financial Transaction Terminal

Referring to Figures 6a, 12a and 12b an embodiment of a RF financial transaction terminal 20 is shown. The RF financial transaction terminal 20 includes an outer casing 22 which accommodates the various components of the DTE 20a and RF modem 20b. A retractable handle 24 depends from the undersurface 22a of the casing 22 to facilitate carrying of the RF financial transaction terminal 20. On the upper top surface of the casing 22 are an LCD display 50, an input keypad 52 and a printer 30 having a spindle carrying a paper roll. A cover is positioned over the printer 30 and has a triangular window on one side (not shown) to allow the condition of the paper roll to be visually determined. The input keypad 52 in this particular example includes a plurality of keys arranged in an array. The rows and columns of the array of keys are scanned in a random order to inhibit false keypad entries and to provide a high tapping resistance. A card reader 38 is partially housed by the casing 22 and has a card reading slot accessible from the rear end of the casing 22.

Although not illustrated, antenna 20c is also mounted on the outer casing 22 and is electrically connected to the RF modem 20b within the casing 22.

The internal components within the casing 22 are best illustrated in Figures 1a, 1b, 12a and 12b. The internal electronic components of the RF financial transaction terminal 20 are mounted on a motherboard 600 and include a main central processing unit (CPU) module 26 which communicates with a secure module 28. The functional division of the internal components into the main CPU module 26 and the secure module 28 is required to provide security, as will be discussed in greater detail herein.

The main CPU module 26 includes a printer interface 32, an RF Tx-Rx interface 36, a card reader interface 40 and a bar code reader interface 44. The main CPU module 26 is also equipped with a main CPU 62 connected to the interfaces 32, 36, 40 and 44 allowing the CPU 62 to control operation of the printer 30, the RF modem 20b, the card reader 38 and the bar code reader 42 (see Figure 9). The CPU 62 is also connected to flash memory 64 and static random access memory (SRAM) 66. The flash memory 64 contains start-up software incorporating a set of routines for initializing the RF financial transaction terminal 20 at power-up. The flash memory 64 also contains a system software loader comprising a routine for downloading system software into the SRAM 66. SRAM 66 contains the system software (eg. interrupt handlers, I/O routines, an application software loader, device drivers etc.), and an applications program area or memory space where a secure prompt table and different applications programs can be downloaded (eg. transaction verification, application specific services, etc.). A solar battery 68 is also provided in the main CPU module 26 for security purposes as will be described and is connected to the main CPU 62.

The secure module 28 provides cryptographic services and security measures to protect the RF financial transaction terminal from software tampering that could result in debit or credit card PIN or passwords from being accessed. The secure module 28 includes a microcontroller unit in the form of a secure chip 48 which controls the operation of the display 50, the keypad 52, a speaker 54, an auxiliary RS-232 port 56 and an interface 58 to the main CPU module 26. The main

CPU module 26 and the secure module 28 receive power from an on-board rechargeable power supply 60 in the usual manner.

Turning to Figure 1b, the secure chip 48 is better illustrated. As can be seen, secure chip 48 includes a CPU 48a, read only memory (ROM) 48b, random access memory (RAM) 48c and interfaces 48d, 48e, 48f, 48g and 56 for the keypad 52, display 50, speaker 54 and auxiliary RS-232 port 56 respectively. The ROM 48b contains a secure chip operating system comprising cryptographic security services, auxiliary RS-232 port control, display control, control of communications to the main CPU module 26 (eg. via MCPUM interface 48d), keypad control and speaker (eg. buzzer) control functions. The RAM 48c is used for cryptographic key storage, password storage, and secure chip operating system working space. The secure chip 48 is preferably in the form of a physically encapsulated secure integrated circuit programmed with the operating system necessary to perform the functions discussed above. The secure module 28 controls the LCD display 50 in a split-screen fashion dividing the LCD display into unsecured and secure display areas. The information displayed in the secure display area is controlled solely by the secure module 28 while the information displayed in the unsecured display area is controlled by the secure module 28 in conjunction with the main CPU module 26 as will be described.

A battery backup 70 (see Figure 1a) is provided to protect against inadvertent power loss and consequent loss of data stored in SRAM 66 and RAM 48c in which the cryptographic keys are stored. Furthermore, ROM 48b is designed so as to prevent unauthorized reading of its content. In addition, since the solar battery 68 is within the casing 22, it is typically isolated from light and does not develop any charge. However, if the integrity of the casing 22 is compromised and the interior of the casing is exposed to light, the solar battery 68 charges. The charge developed by the solar battery 68 is sensed by the main CPU 62 which in turn clears the cryptographic keys stored in the RAM 48c to prevent an intruder from acquiring the cryptographic keys.

Turning now to Figures 6a to 13, mechanical aspects of the RF financial transaction terminal 20 will now be discussed. Figure 6a shows the RF financial transaction terminal 20 in perspective and as can be seen, the handle 24 is received in a recess 100 formed in the underside 22a of the casing 22. Fasteners in

the form of screws 102 secure the handle to the casing 22 allowing the handle 24 to be removed from the casing 22. The battery 60 is received in a pocket (not shown) formed in the underside 22a of casing 22. A multi-pin electrical connector 104 forming part of the bar code reader interface 44 is hidden by a cover 106 and is also located on the underside 22a of casing 22.

Figures 6b to 6e and 7 better illustrate the handle 24. As can be seen, the handle 24 includes upper and lower handle sections 140 and 142 respectively which are rotatable relative to one another to allow the handle to move between an extended pistol grip position and a retracted palm grip position (see Figure 7). The lower handle section 140 is hollow and is constituted by a pair of mating halves 144 and 146 respectively retained together by fasteners 148 (only one of which is shown). The lower handle section has an oblique obround surface 150 in which a square recess 152 is formed. A circular aperture 154 is provided in the center of the bottom surface 156 of the recess 152 while a pair of diametrically opposed stops 160 project upwardly from the bottom surface 156. Beneath the recess 152 and adjacent opposed interior side walls of the lower handle section 140 are U-shaped retainers 158.

Within the lower handle section 140 is part of a handle rotating mechanism 162. As is best seen in Figure 6c, rotating mechanism 162 includes a support 164 through which one of the fasteners 148 passes to secure its position within the lower handle section 140. A cylinder 166 projects from the support 164 and passes through the apertures formed in the bottom surface 156 and obround surface 150 respectively. On the cylinder 166 adjacent the support are a pair of spaced annulets 168 and 170 respectively. The annulet 168 closest to the support 164 is positioned below the bottom surface 156 and has a pair of diametrically opposed projecting tabs 172 formed on it. The tabs 172 are received by the retainers 158 to inhibit relative rotation of the handle rotating mechanism 162 and the lower handle section 140. The other annulet 170 is positioned above the bottom surface 156 and is accommodated within the recess 152. The annulets 168 and 170 have diameters greater than that of the aperture 154.

The upper handle section 142 (best seen in Figures 6d and 6e) is also hollow and is constituted by a pair of mating halves 180 and 182 retained together by fasteners 183. The upper handle section also has an oblique obround surface 184

which overlies obround surface 150. A sleeve 186 depends from surface 184 and accommodates a portion of cylinder 166. The sleeve 186 extends into the recess 152 and has a projecting tab 188 on it which abuts the stops 160 to limit relative rotation of the two handle sections 140 and 142 respectively to 180 degrees.

The sleeve 186 also extends into the upper handle section 142 and has a surface 190 in which an aperture 192 is provided to allow the cylinder 166 to pass. An annulet 194 is formed at the distal end of the cylinder 166 and has a diameter greater than that of the aperture 192. The annulet 194 has a pair of diametrically opposed notches 195 formed in it which communicate with a latch 196 to retain the handle 24 in one of the extended pistol grip or retracted palm grip positions. The latch has trunnions 197 on it which are accommodated by hollow cylinders 198 extending from the side walls of the upper handle section 142. The latch 196 includes a manually operable release 200 which projects through an opening 202 in the upper handle section 142 as well as a retaining arm 204. A spring 206 biases the retaining arm 204 of latch 196 to urge it against the annulet 194. A pair of inwardly projecting posts 208 inhibit lateral movement of the latch 196 within the upper handle section 142.

An attachment plate 210 is secured to the upper handle section 142 by fasteners 212 (only one of which is shown) which are accommodated in threaded receptacles 214. The plate 210 is accommodated by the recess 100 in the casing 22 and is secured to the casing 22 by the fasteners 102.

In use, when the handle 24 is in either the pistol grip or retracted palm grip position, the retaining arm 204 of latch 196 is urged into one of the notches 195 formed in the annulet 194. Rotation of the lower handle section relative to the upper handle section is inhibited. When the manually operated release 200 is pushed, the retaining arm 204 pivots against the bias of the spring 206 to bring the retaining arm 204 out of the notch 195. Rotation of the lower handle section 140 relative to the upper handle section 142 is then permitted but only in one direction due to the fact that the projecting tab 188 on the sleeve 186 abuts one of the stops 160.

Once the lower handle section 140 has been rotated to bring the retaining arm 204 out of alignment with the notch 195, the release 200 can be released. The retaining arm 204 is urged by the spring 206 toward the annulet 194

but because the retaining arm 204 runs along the outside surface of the annulet 194 it does not prevent the lower handle section 140 from rotating. As the lower handle section 140 is further rotated, the other notch 195 becomes aligned with the retaining arm 204 and the retaining arm snaps into the notch 195 inhibiting any further relative rotation of the upper and lower handle sections. If the release 200 is held, continued relative rotation of the upper and lower handle sections in the same direction is inhibited due to the fact that the projecting tab 188 on the sleeve 186 will abut the other stop 160. The upper and lower handle sections 142 and 140 can be moved back to their previous positions by pivoting the retaining arm 204 once again by actuating the release 200 and rotating the lower handle section 140 relative to the upper handle section 142 in the opposite direction.

Referring now to Figure 8, a portion of the interior of the casing 22 is better illustrated. As can be seen, the casing 22 has an interior support surface 220 with four generally rectangular openings 222 provided in it which are aligned with the fasteners 102 extending through the attachment plate 210. The support surface 220 supports a card reader mounting frame 224. The mounting frame 224 has a base plate 226 which overlies the support surface 220. The base plate 226 has four punches 228 in it adjacent its corners which are received in complimentary openings 222 formed in the support surface 220. The fasteners 102 pass through the openings 222 and threadably engage with apertures 230 in the punches 228. Fasteners 232 also pass through apertures 233 in the base plate 226 and engage with apertures 234 in the support surface 220.

Sidewalls 240 extend along opposed majors sides of the base plate 226. A bridge 242 spans the sidewalls 240 and is spaced above the base plate 226. The card reader 38 is accommodated between the sidewalls and is supported by the sidewalls 240 and bridge 242. Fasteners 244 pass through apertures 246 in the sidewalls 240 and are accommodated by apertures 248 in the card reader 38 to secure the card reader to the mounting frame 224.

The sidewalls 240 and bridge 242 are designed to inhibit shocks from being applied to the card reader 38 in the event that the RF financial transaction terminal 20 is dropped or collides with another object. Specifically, the sidewalls 240 and bridge 242 are formed of aluminum and are dimensioned so that they are able to

flex approximately 1.2mm due to the extensile structure of the sidewalls 240. Therefore, in the event of a shock being applied to the RF financial transaction terminal 20, the sidewalls 240 and bridge 242 flex and act as a shock absorber for the card reader 38 so that the card reader floats within the casing 22.

In normal operation of the RF financial transaction terminal, the secure module 28 operates in conjunction with the main CPU 62 in the CPU module 26 as the main CPU 62 executes the applications program to allow transactions to be entered at the location of a user and conveyed over the RF communications link to the central network controller 12 as well as to receive transaction verification data from the host computers at the financial institution via the central network controller 12 and the RF communications link.

During this operation, as the main CPU 62 executes the applications program, the CPU 62 must request the services of the secure module 28 via interface 58 whenever data needs to be displayed on the LCD display 50 or entered via the input keypad 58. The secure module 28 recognizes three different types of requests generated by the main CPU 62, namely a "display only" request, a "display prompt" request and a "display secure prompt" request.

The display only and display prompt requests are typically generated by the main CPU 62 when the RF financial transaction terminal is used in normal operation and transactions are being carried out at user locations. Display secure prompts are generated by the host computers at financial institutions and are the most sensitive due to the fact that keyboard entries are passed to the main CPU module 26 in clear text form.

When the secure module 28 receives a display only request from the main CPU 62, the secure module 28 causes the word "UNSECURED" to flash in the secure display area of the LCD display 50 and displays keypad entries on the unsecured display area without checking the data. The keypad entries are not forwarded to the main CPU module 26. Presses of the entry key of the keypad 52 are however passed to the main CPU 62 by the secure module 28 to signal the main CPU to proceed with the applications program.

When the secure module 28 receives a display prompt request from the main CPU 62, the secure module causes the word "SECURE" to be continuously

displayed in the secure display area of the LCD display 50 and displays the appropriate prompt such as "Enter PIN" on the unsecured display area of the LCD display 50. Keypad entries are encrypted by the secure chip 48 in the secure module 28 before being conveyed to the main CPU 62 and are not displayed.

Thus, during normal operation transaction data which is to be forwarded to the host computers at the financial institution is not displayed on the LCD display 50 when entered and is encrypted prior to being transmitted over the RF communications link to provide proper security.

When the secure module 28 receives a display secure prompt request from the main CPU 62, the secure module requests the main CPU to provide a prompt authentication code (PAC) associated with the secure prompt being requested. The PACs are generated by the host computers in the financial institutions using a cryptographic algorithm for each secure prompt and are transmitted to the RF financial transaction terminals by the host computers when the RF financial transaction terminal is physically connected to the central network controller 12 as will be described.

When the secure module receives the secure prompt request together with the PAC, the secure chip 48 compares the PAC with the content of a secure prompt table in RAM 48c. If the results of the comparison are proper, the secure module 28 passes entries made using the keypad 52 directly to the main CPU 62 in clear text form. If the results of the comparison are not correct, the secure module 28 denies the secure prompt request.

Central Network Controller

Referring now to Figure 2, the central network controller 12 is better illustrated. The network central controller 12 is typically located in a retailer's premises and is powered by a power supply 80 connected to AC mains. The central network controller is also connected to a dial-up or leased-line phone cable. The central network controller 12 includes a CPU motherboard with a main microprocessor 82 and associated memory 84. The main microprocessor 82 is connected to a RF transceiver 86 in the form of a RF modem having an antenna 88 for establishing a RF communications link with the various RF financial transaction terminals 20 using a wireless data communications network. A DATAPAC interface

90 is provided with DATAPAC 3101 and 3201 surface interfaces. An ISDN interface board may also optionally be provided. A serial RS-232 interface 92 is included in the central network controller 12 to allow updates to data and software used by the RF financial transaction terminals 20 and central network controller 12 to be downloaded. A serial RS-485 interface 94 is also provided for optional connection of the central network controller 12 to the retailer's existing point-of sale platforms.

The central network controller 12 functions as a gateway between the RF financial transaction terminals 20 and the standard interfaces (ie. DATAPAC) leading to the host computers at financial institutions. The central network controller 12 forms a transparent link for all transaction requests generated by the RF financial transaction terminals that are conveyed to financial institutions as well as for all replies generated by financial institutions that are conveyed to the RF financial transaction terminals 20 in response to received transaction requests.

The memory 84 stores software which is executed by the main microprocessor 82 allowing the central network controller 12 to perform a number of functions. Specifically, the central network controller 12 effects wireless data communication network control using a communications protocol, discussed in greater detail below. The central network controller 12 also controls message exchange between the RF financial transaction terminals and the financial institutions. Specifically, the central network controller 12 collects transaction requests from the individual RF financial transaction terminals 20 and forwards them to the host computers at the appropriate financial institutions in order the transaction requests are received. In addition, the central network controller 12 controls message exchange between the central network controller 12 and the host computers at financial institutions using DATAPAC 3101 or DATAPAC 3201 services. The central network controller 12 supports existing data communications protocol as defined by Telecom Canada. However, if desired an ISDN interface can be used instead of the DATAPAC 3101 and 3201 services.

The central network controller 12 also receives and stores new RF financial transaction terminal software releases and new RF financial transaction terminal secure prompt tables provided by the financial institution for use in the RF financial transaction terminals. For example, a financial institution can download the

new RF financial transaction terminal software to the central network controller 12 via the RS-232 interface 92 for storage in memory 84. The central network controller 12 can then download the updated software to the RF financial transaction terminals to update them by way of a physical serial cable connection established between the RS-232 interface 92 of the central network controller 12 and the RS-232 interfaces 56 on the RF financial transaction terminals 20. When the software in all of the RF financial transaction terminals has been updated, the new RF financial transaction terminal software can be deleted from the memory 84. The central network controller 12 also controls communication with the existing point-of-sale platforms at the retailer location via the serial RS-485 interface 94. This allows a retailer to use existing cash registers to exchange data such as prices, totals, etc. to the central network controller 12.

Prior to operation of the financial transaction system 10, the central network controller 12 is put through an initialization routine to establish several configuration parameters. The initialization routine will now be described.

Central Network Controller Initialization

During initialization, one of the RF financial transaction devices is physically connected to the central network controller 12 by way of a serial cable connected to the RS-232 interfaces 56 and 92 respectively to allow the keypad 52 of the RF financial transaction device to be used to enter data into the central network controller 12. The keypad 52 is used to enter or select the following:

i) The current time and date;

ii) The type of communications format to be used to communicate with the host computers at the financial institution;

iii) The type of point-of-sale platform at the retailer's location to be connected to the RS-485 interface 94;

iv) The telephone number of the modem at the financial institution that should be dialled to request download of new RF financial transaction terminal software;

v) The telephone number of the modem at the financial institution that should be dialled to request download of a new RF financial transaction terminal secure prompt table;

vi) Telephone numbers and network addresses for credit and debit transactions; and

vii) The destination addresses of the RF financial transaction terminals in the financial transaction system 10.

Following this, the RF financial transaction terminal software and secure prompt table must be downloaded to the central network controller 12 from the financial institution. During this stage of the initialization, the host computer at the financial institution contacts the central network controller 12 using a dial-up modem and transmits a message indicating the type of data to be downloaded to the central network controller 12 ie. the RF financial transaction terminal software or the secure prompt table. Once the message has been transmitted to the central network controller, the connection is terminated. The central network controller 12 then establishes a connection to the financial institution by dialling the appropriate modem number initialized at either step iv or v above. Once the connection is established, the RF financial transaction terminal software or secure prompt table is downloaded into the memory 84 of the central network controller 12.

Following this, each RF financial transaction terminal 20 is connected to the central network controller 12 via a serial cable connected between the RS-232 interfaces 56 and 94 respectively so that the RF financial transaction terminal software or secure prompt table can be downloaded into the RF financial transaction terminal. The download procedure is initiated using the keypad on the RF financial transaction terminal. After the RF financial transaction terminal software or secure prompt table has been downloaded, the RF financial transaction terminal is prompted by the financial institution to generate a Download Request-Terminal Initialization transaction which is conveyed to the financial institution by way of the central network controller 12 in order to synchronize the cryptographic keys stored therein and to receive operational parameters from the financial institution. Also, depending on information required by the financial institution, the financial institution may pass an instruction to the RF financial transaction terminal which causes the main CPU 62 to generate a secure prompt request.

Once the above has been done, the connection between the central network controller and the host computer at the financial institution can be

terminated. As should be appreciated, the above steps are performed separately in order to initiate download of the RF financial transaction terminal software and secure prompt table and are performed for each RF financial transaction terminal 20 in the financial transaction system 10.

Communications Protocol

As mentioned previously, the RF financial transaction terminals 20 and the central network controller 12 use a communications protocol to exchange data over the RF communications link. The communications protocol will now be described.

Messages and Packets

In the communications protocol, a number of types of messages are generated either by the MCU in the RF modem 20b or 86 or by the DTE 20a. Depending on the type of message, different operations are performed. The messages generated in the communications protocol of the present invention are information messages (i_messages), command messages (comm.msg), error messages (error_message) and acknowledgement messages (ack_messages).

Information and command messages are generated by a DTE 20a and are conveyed to the MCU in the RF modem. Information messages are messages which are to be transmitted on the RF communications link and are addressed to a particular RF financial transaction terminal 20 or to the central network controller 12. When a RF modem receives an information message it adds a data link (DLL) layer to it to create an information packet (i_packet) before transmitting the i_packet on the RF communications link.

A command message is a message which is to be used by the RF modem for internal purposes to reset command parameters therein. A command message is not put in the form of an i_packet by the RF modem and therefore, is not transmitted on the RF communications link.

Error messages are generated by the MCU in a RF modem in the event that proper communications cannot be established over the RF communications link. Error messages generated by the MCU are conveyed to the DTE.

Acknowledgment messages are generated by the MCU of a RF modem after an i_packet has been properly received. The MCU then adds a DLL layer to

the acknowledgement message to create an acknowledgement packet (ack_packet) before transmitting the ack_packet on the RF communications link addressed to the RF financial transaction terminal or central network controller that sent the received i_packet.

There are two types of incoming packets that a MCU can receive on the RF communications link, namely, an i_packet and an ack_packet. An i_packet received by a RF modem is forwarded to the DTE in the form of an i_message (after stripping the DLL header from it) if it is error free, and if the destination address of the i_packet is valid. An ack_packet received by a RF modem is not forwarded to the DTE. Appendix A better illustrates the form of the various packets and messages generated using the communications protocol.

Messaging

The communications protocol provides for three modes of operation, namely an idle mode, a transmit (Tx) mode and a receive (Rx) mode. The following is a description of the idle, receive and transmit modes of operation of the RF financial transaction terminals 20 and the central network controller 12 with reference to Figures 4 and 5.

RF modem Initialization

When a RF financial transaction terminal 20 or the central network controller 12 is powered up or reset (block 700), the MCU of the RF modem initiates a startup procedure (block 702). During this procedure, the MCU resets an acknowledge flag (ack_ok_flg) to 0 and sets an acknowledge timer (ack_timer) to an initial value (ack_a_init). At this stage, the acknowledge timer starts counting down and when the acknowledge timer expires, the acknowledge flag (ack_ok_flg) is set to 1. Once the startup procedure 702 has been completed, the MCU of the RF modem enters an idle mode (block 704).

Idle mode

In the idle mode, the MCU of the RF modem waits to be interrupted by either an RTS signal received from the DTE, an incoming packet received on the RF communications link or an expired timer signal.

Rx mode

If an incoming packet is received by the RF modem on the RF communications link (block 710), the MCU removes the DLL header from the incoming packet and calculates a cyclic redundancy check (CRC) value (block 712). The calculated CRC value is then checked to determine if it is valid (block 714). If the CRC value is not valid, the MCU resets the acknowledge timer to the initial value (ack_a_init) and sets the acknowledge flag (ack_ok_flg) to 0 (block 716) before returning to the idle mode (block 718). If at block 714 the CRC value is determined to be valid, the destination address (dest_id) of the incoming packet is checked (block 720). If the destination address is not valid, the MCU proceeds to block 716.

If the destination address is valid, the incoming packet is checked to determine if it is an i_packet (block 722). If the incoming packet is determined not to be an i_packet, then it is then checked to determine if it is an ack_packet (block 724). If the incoming packet is determined not to be an ack_packet, the MCU proceeds to block 716. If the incoming packet is an ack_packet, the MCU sets the

A financial transaction system is provided in which a user is given a portable RF financial transaction terminal with which to enter transaction data via a keypad or read a UPC bar code on merchandise via a CCD scanner and read their credit, debit or smart card. The RF financial transaction terminal transmits the transaction and card data to a central network controller via a RF communications link. The central network controller in turn conveys the transaction and card data to the host computers at a financial institution where the transaction is processed in real-time. The financial institutions return verification data to the central network controller which is passed back to the RF financial transaction terminal via the RF communications link. The RF financial transaction terminal then generates a printed receipt of the transaction for the user. All of this may be done while the RF financial transaction terminal and the user's credit, debit or smart card remains in the total custody of the user. The user is therefore relieved from having to proceed to an ABM, retail platform, cashier's desk, etc. acknowledge flag (ack_ok_flg) to 1 (block 725) before proceeding to block 718.

If at block 722 the incoming packet is determined to be an i_packet, the MCU forwards the i_message to the DTE (block 726). The MCU then causes the

RF modem to generate and transmit an ack_packet on the RF communications link addressed to the RF modem of the RF financial transaction terminal or central network controller that sent the i_message to confirm receipt of the i_message (block 728). Following this, the MCU proceeds to block 718 and enters the idle mode.

Tx mode

If the MCU receives an RTS signal (block 730), the MCU is conditioned to the transmit mode and awaits receipt of a message from the DTE (block 732). When the message is received from the DTE, the MCU checks the message to determine if it is a comm_message (block 734). If the message is a comm_message, the MCU resets the communications parameters (comm.params) therein in accordance with the comm_message (block 736) before returning to the idle mode (block 738).

If at block 734 the message is determined not to be a comm_message, the message is assumed to be an i_message. The MCU in turn calculates and adds the DLL header to the i_message to create an i_packet (block 740). Once the i_packet has been created, the MCU checks to determine if the acknowledge flag (ack_ok_flg) is set to 1 (block 742). If the acknowledge flag is not set, the MCU returns to an idle mode (block 744) and waits for the acknowledge flag (ack_ok_flg) to be set to 1. At block 742 if the acknowledge flag is set, the MCU calculates a random number k (block 746), sets a network access denied timer (nad_timer) to an initial value equal to k * nad_d where nad_d is equal to 8.5ms (block 748) before returning to an idle mode (block 750) waiting for the nad_timer to expire. In the idle mode at block 744, the MCU waits for the acknowledge flag (ack_ok_flg) to be set to 1 as shown at block 752, and then proceeds to block 746. The generated random number k is of the form $k \in 16,31$ if the i_message is being originally transmitted and is of the form $k \in 0,15$ if the i_message is being retransmitted. The nad_timer is used to provide randomization of RF communications link channel occupation attempts.

When the nad_timer expires (block 754), the MCU sets a transmission counter (R_Tx_CNT) to an initial value (R_Tx_NMB) representing the number of times the RF modem will attempt to transmit a packet (block 756). Once the transmission counter has been set, the RF modem transmits the packet on the RF communications link, decrements the transmission counter (R_Tx_CNT) by one and

sets an acknowledge response timer (R_Tx_Timer) to an initial value (R_Tx_D) (block 758). In this particular example, the initial value (R_Tx_D) is equal to the initial value of the acknowledge timer, namely ack_a_init. Following this, the MCU enters an idle mode (block 760).

After the packet is transmitted on the RF communications link, the MCU awaits receipt of an ack_packet from the RF financial transaction terminal 20 or central network controller 12 to which the packet was addressed to confirm that the packet was properly received. If the acknowledge response timer (R_Tx_Timer) expires before the ack_packet is received (block 762), the MCU checks the value of the transmission counter (R_Tx_CNT) (block 764). If the value of the transmission counter is equal to zero, the MCU sends an error message to the DTE 20a to inform that DTE 20a that the packet was not successfully transmitted (block 766) and the MCU returns to the idle mode (block 768). If at block 764 the value of the transmission counter is determined to be greater than zero, the MCU proceeds to block 746 and the following steps are performed again in order to retransmit the packet.

Acknowledge and Acknowledge Response Timers

After transmission of a packet on the RF communications link, it is necessary for the MCU to allow the RF financial transaction terminal or central network controller to which the packet was sent sufficient time to respond with an ack_packet without interruption by other MCUs. This is done by setting the acknowledge and acknowledge response timers (ack_timers and R_Tx_Timers) in all RF modems to a predetermined initial value (ack_a_init) after an incoming packet with a valid CRC and destination address (dest_id) is received. The ack_a_init value must be large enough to ensure that a RF modem will have sufficient time to receive the packet, check the CRC value, remove the DLL header, forward the i_message to the DTE, create an ack_ packet and send it to the transmitting MCU before the timers expire.

In the present financial transaction system 10, the ack_a_init value is given by:

2 x prop_delay+MCU_Rx_pr+RF modem_TO_DTE_transf+MCU___ack_pr +ACK_xmit+T_ambg

where:

prop_delay is the packet transmission propagation delay and is assumed to be approximately equal to 0;

MCU_Rx_pr is the time needed for the MCU to process the received packet;

RF modem_to_DTE_transf is the time needed for the MCU to transfer the i_message to the DTE;

MCU_ack_pr: is the time needed for the MCU to generate the ack_packet;

ACK_xmit is the ack_packet transmission time; and

T_ambg is ambiguity time added to the ack_a_init value to provide a buffer.

Referring now to Figure 9, another embodiment of the RF financial transaction terminal 20 is shown. In this embodiment, the handle 24 is replaced with a CCD unit bar code reader 42. As can be seen, the bar code reader 42 includes a body 300 with a plate 302 on it which is basically the same size as plate 210 and which is received by the recess 100 formed in the casing 22. Fasteners 102 pass through apertures 304 in the body 300 and threadably engage the apertures 230 in the punches 228. A pair of wings 310 extend from the sides of the body 300. Fasteners 312 pass through apertures 314 in the wings 310 and threadably engage apertures 315 in the underside 22a of the casing 22. A conventional CCD scanner (not shown) is housed within the body. The front of the body includes a pane 316 through which the laser beam generated by the CCD scanner can pass so that bar codes can be read. On the upper surface of the body 300 is a multi-pin electrical connector (not shown) which mates with the complimentary electrical connector 104 on the underside 22a. A pistol grip handle 318 depends from the body 300 and has a manually operable trigger 320 on it which when actuated operates the CCD scanner.

When the bar code reader 42 is to be used, the fasteners 102 attaching the handle 24 to the casing 22 are loosened and the handle 24 is removed. The cover 106 over the electrical connector 104 on the radio terminal 20 is also removed to expose it. The bar code reader 42 is then attached to the casing 22 via fasteners 102 and 312. At this time, the electrical connectors mate and power is supplied to the bar code reader 42 by the battery 60. Logic in the bar code reader 42 detects when the bar code reader is connected to the battery and automatically powers the bar code

reader so that it becomes operative. The bar code reader then operates in a conventional manner with the CCD scanner generating a laser beam which passes through the pane 316 when the trigger 320 is actuated. When the laser beam is scanned across a bar code, the CCD scanner reads the scanned bar code and conveys the information to the RF financial transaction terminal 20 via interface 44 in a conventional manner to record the transaction data.

With reference to Figure 10, a charging dock 400 is shown for receiving the RF financial transaction terminal 20 when the handle 24 is in the retracted position. A non-contact charger unit is accommodated by a charging dock cavity 401 within the dock 400 for charging the power supply 60. A charging stud 402 on the dock is received by a charging receptacle 404 formed in the undersurface 22a of casing 22 to properly position the RF financial transaction terminal 20 within the dock so that charging of the power supply can occur.

Figure 11 shows a charging and carrying nest 500 for carrying the RF financial transaction terminal 20 when the handle 24 is in the extended pistol grip position. The charging and carrying nest 500 also includes a charging stud 402 to register with the charging receptacle 404 formed in the undersurface of the casing 22.

In both the charging dock 400 and charging nest 500, the rear case of the dock or nest is built-up. This is done to prevent the RF financial transaction terminal 20 from being placed in the dock or nest when a card is positioned in the card reader or from trying to insert a card into the card reader when the RF financial transaction terminal is being charged. This design helps to inhibit the erasure of data recorded on the magnetic strip of a credit or debit card by the fields created by the dock or nest.

Figure 13 shows yet another embodiment of a handle for the RF financial transaction terminal 20. In this embodiment, the handle 24 is connected to the undersurface 22a of casing 22 by means of a tongue 650 cooperating with an internal slot 652 formed in the undersurface 22a of casing 22, and a pair of one-way screws 654. The handle 24 is formed in a single piece construction and therefore, remains in the extended pistol grip position.

Although the card reader has been described to read credit or debit cards, it should be apparent to those of skill in the art that a smart card reader having read/write functions may be incorporated into the RF financial transaction terminal.

Although various embodiments of RF financial transaction terminals have been described for use in a financial transaction system, those of skill in the art will appreciate that variations and modifications may be made to the present invention without departing from the scope thereof as defined by the appended claims.

APPENDIX A

The following is a description of the various message and packet formats:

i_packet

|synch|CRC[2]|DLL_ctrl[1]|'STX'|msg_type[1]|dest_id[1]|source_id[1]| data [123]|'ETX' or 'ETB'|

where:

i_message starts at 'STX' and ends at 'ETX' or 'ETB'; and

DLL header consists of 16 bit cyclic redundancy check value (synch CRC) and a DLL control byte (DLL_ctrl).

In the i_message:

i) the position of the destination and source identifications (dest_id and source_id) are fixed;

ii) the maximum number of data bytes is set at 123; and

iii) STX and ETX or ETB bytes only appear at beginning and end of i_message.

The DLL control byte has the following format:

-QQQQSSSS where:

QQQQ is request type: 1000 for information and 0111 for ack_packet

SSSS is presently unused

ack_packet

|synch|CRC[2]|DLL_ctrl[1]|'STX'|msg_type[1]|dest_ID[1]|source_ID[1]| 'ETX'|

APPENDIX A - CON'T

Control message

|'STX'|msg_type[1]|dest_ID[1]|source_ID[1]|'ETX'|

Error message

|'STX'|msg_type[1]|dest_ID[1]|source_ID[1]error_code[1]|'ETX'|

What is claimed is:

1. A portable radio frequency financial transaction terminal comprising:

a housing;

input means to allow transaction data to be entered therein;

a card reader to receive and read credit, debit or smart card;

a processor in communication with said input means and said card reader to receive and process transaction and card data; and

a radio frequency transmitter to transmit said transaction and card data to a remote site whereat a transaction can be processed.

2. A terminal as defined in claim 1 further comprising a radio frequency receiver to receive verification data from said remote site that said transaction has been verified and processed.

3. A terminal as defined in claim 2 further comprising a printer to generate a printed receipt of said transaction.

4. A terminal as defined in claim 3 wherein said printer is inhibited from generating said receipt until said receiver has received said verification data.

5. A terminal as defined in claim 4 wherein said input means includes a keypad and/or a bar code reader to allow said transaction data to be entered.

6. A terminal as defined in claim 1 wherein said processing means includes cryptographic security to encrypt said transaction and card data prior to transmission.

7. A terminal as defined in claim 6 further comprising tamper proof means to inhibit access to cryptographic data used by said cryptographic security.

8. A terminal as defined in claim 7 wherein said tamper-proof means includes a solar battery within said housing, said solar battery developing a charge when exposed to light signifying unauthorized access into said housing, said processor detecting charge developed by said solar battery and deleting said cryptographic data to inhibit unauthorized access thereto.

9. A terminal as defined in claim 1 wherein said housing has a pistol grip to facilitate carrying thereof.

10. A terminal as defined in claim 9 wherein said pistol grip is movable between extended and retracted positions.

11. A terminal as defined in claim 10 wherein said pistol grip includes a locking mechanism to maintain said pistol grip in one of said extended and retracted positions and a release to release said locking mechanism to allow said pistol grip to be moved between said extended and retracted positions.

12. A terminal as defined in claim 5 wherein said bar code reader is removably attachable to said housing.

13. A terminal as defined in claim 1 further comprising shock absorbing means acting between said card reader and said housing to inhibit shocks from being applied to said card reader.

14. A financial transaction system comprising:

a plurality of portable radio frequency financial transaction terminals to receive transaction and debit, credit or smart card data; and

a central network controller in communication with each of said portable radio frequency financial transaction terminals via a RF communications link, said central network controller receiving said transaction and card data transmitted by said portable radio frequency financial transaction terminals and conveying said

transaction and card data to a financial institution whereat transactions can be processed.

15. A system as defined in claim 14 wherein said central network controller receives verification data from said financial institution that said transactions are valid, said central network controller transmitting said verification data to said portable radio frequency financial transaction terminals via said RF communications link to confirm valid transactions.

16. A system as defined in claim 15 wherein data transmitted over said RF communications link is encrypted.

17. A financial transaction terminal comprising:

a housing;

input means to allow transaction data to be entered therein;

a card reader to receive and read credit, debit or smart cards;

a processor in communication with said input means and said card reader to receive and process transaction and card data; and

shock absorbing means acting between said card reader and said housing to inhibit shocks from being applied to said card reader.

18. A terminal as defined in claim 17 wherein said shock absorbing means includes a frame having a pair of flexible, laterally spaced walls and a flexible transverse bridge extending between said walls, said card reader resting on said bridge and being positioned between said walls; and fastening means to secure said card reader to said walls.

19. A financial transaction terminal comprising:

a housing;

input means to allow transaction data to be entered therein;

a card reader to receive and read credit, debit or smart cards;

a processor in communication with said input means and said card reader to receive and process transaction and card data; and

a pistol grip depending from said housing to facilitate carrying of said terminal, said pistol grip being movable between extended and retracted positions.

20. A terminal as defined in claim 19 wherein said pistol grip includes a locking mechanism to maintain said pistol grip in one of said extended and retracted positions and a release to release said locking mechanism to allow said pistol grip to be moved between said extended and retracted positions.

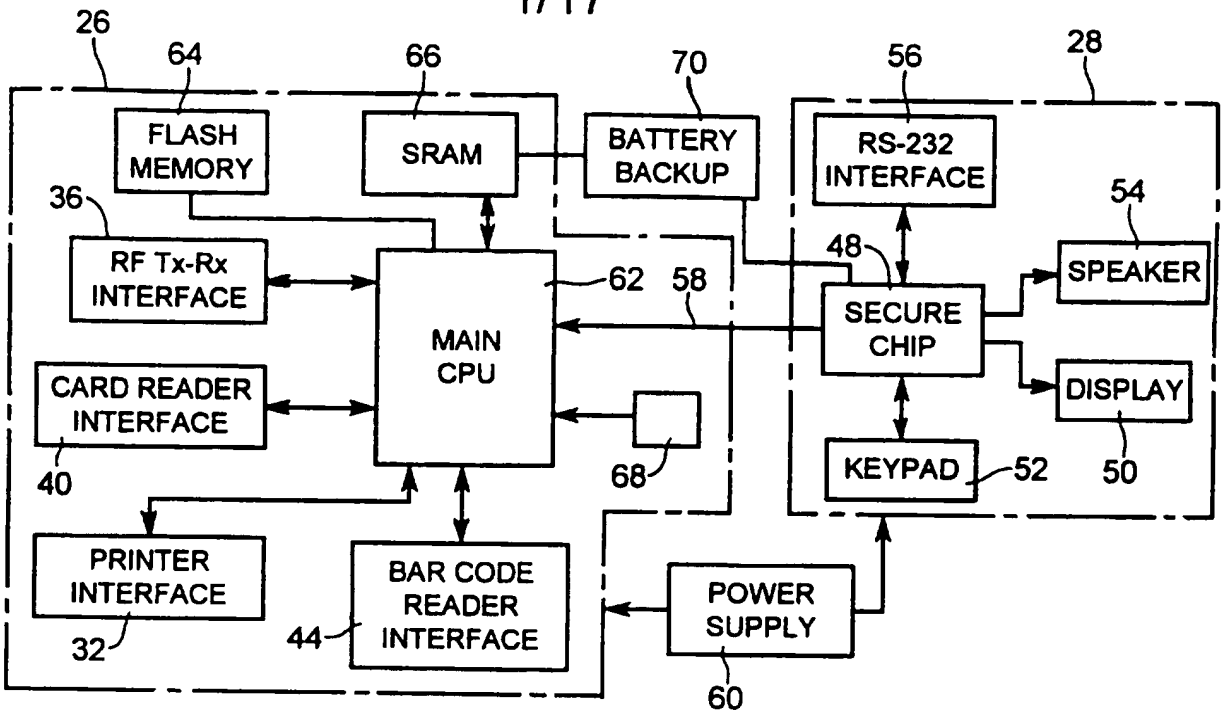

26
64
66
70
56
28
FLASH MEMORY
SRAM
BATTERY BACKUP
RS-232 INTERFACE
36
54
RF Tx-Rx INTERFACE
48
SPEAKER
62
58
MAIN CPU
SECURE CHIP
CARD READER INTERFACE
DISPLAY
40
68
KEYPAD
52
50
PRINTER INTERFACE
BAR CODE READER INTERFACE
POWER SUPPLY
32
44
60

FIG. 1a

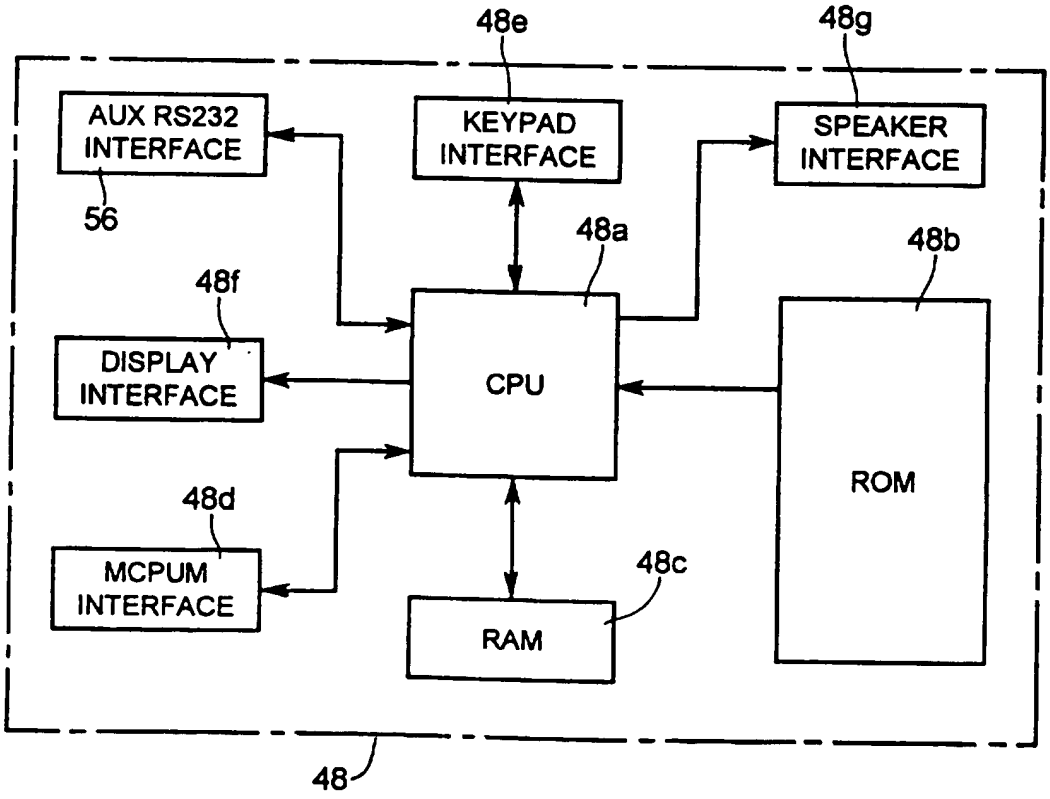

48e
48g
AUX RS232 INTERFACE
KEYPAD INTERFACE
SPEAKER INTERFACE
56
48a
48b
48f
DISPLAY INTERFACE
CPU
ROM
48d
MCPUM INTERFACE
48c
RAM
48

FIG. 1b

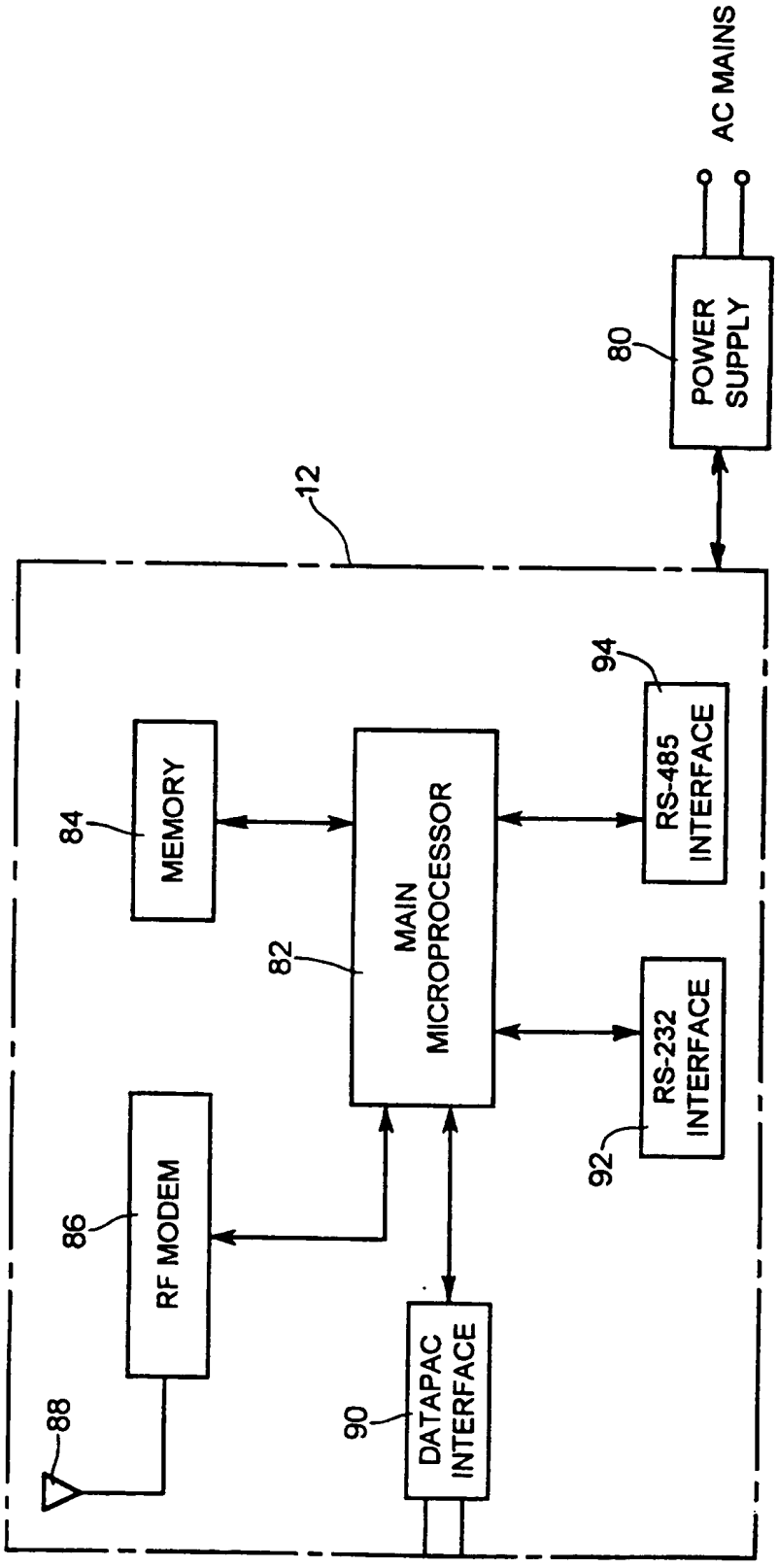

AC MAINS
POWER SUPPLY
80
12
MEMORY
84
MAIN MICROPROCESSOR
82
RS-485 INTERFACE
94
RS-232 INTERFACE
92
RF MODEM
86
88
DATAPAC INTERFACE
90

FIG. 2

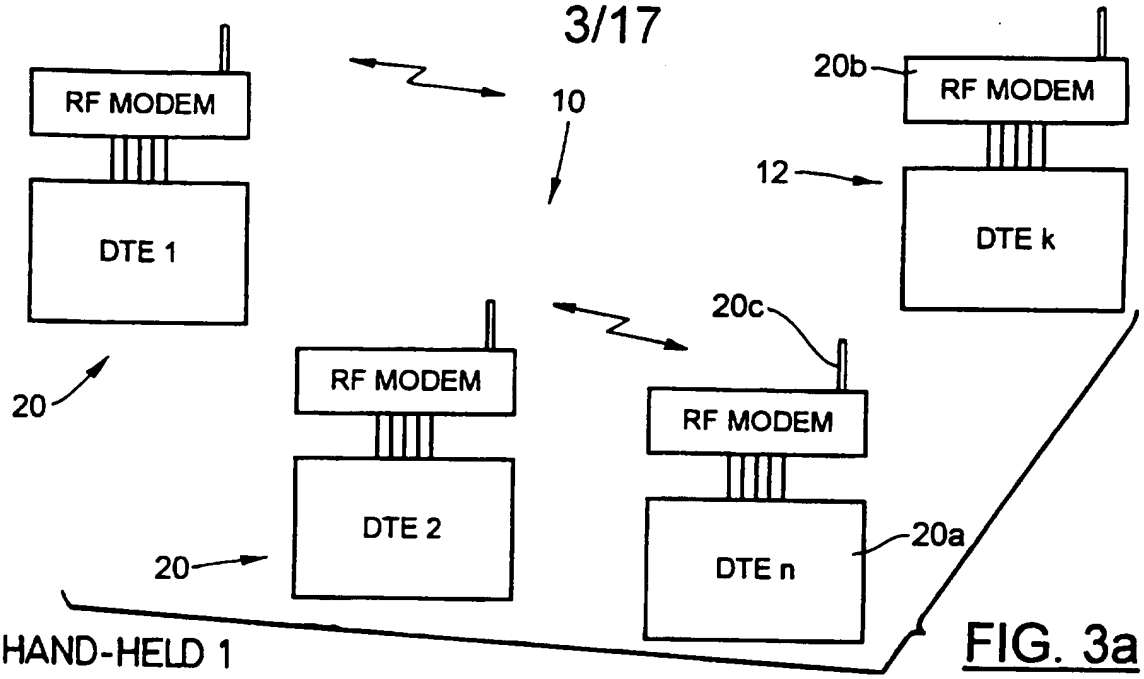

RF MODEM
DTE 1
10
20b
RF MODEM
12
DTE k
20c
RF MODEM
RF MODEM
DTE 2
DTE n
20
20
20a

FIG. 3a

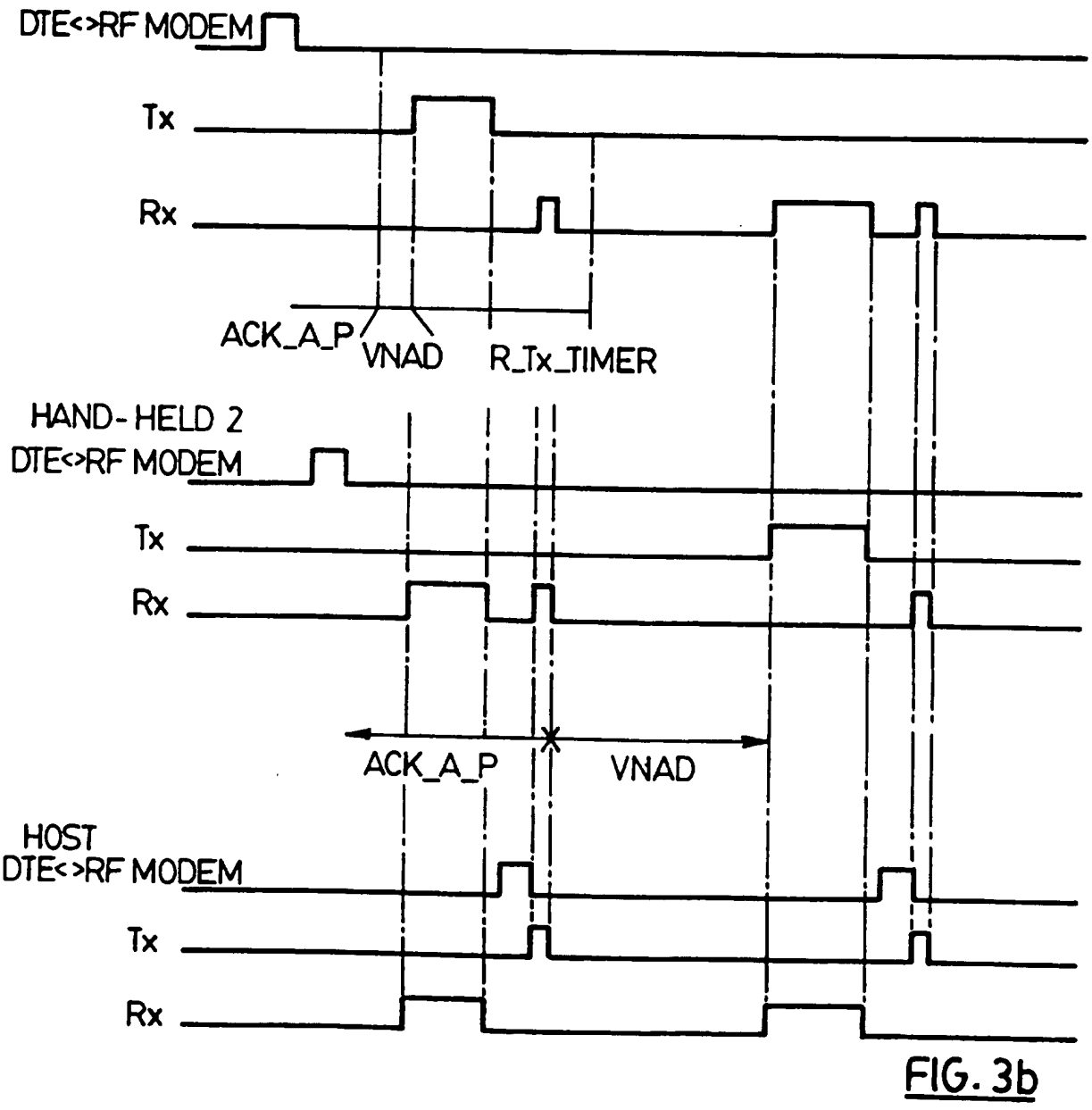

HAND-HELD 1
DTE<>RF MODEM
Tx
Rx
ACK_A_P
VNAD
R_Tx_TIMER
HAND-HELD 2
DTE<>RF MODEM
Tx
Rx
ACK_A_P
VNAD
HOST
DTE<>RF MODEM
Tx
Rx

FIG. 3b

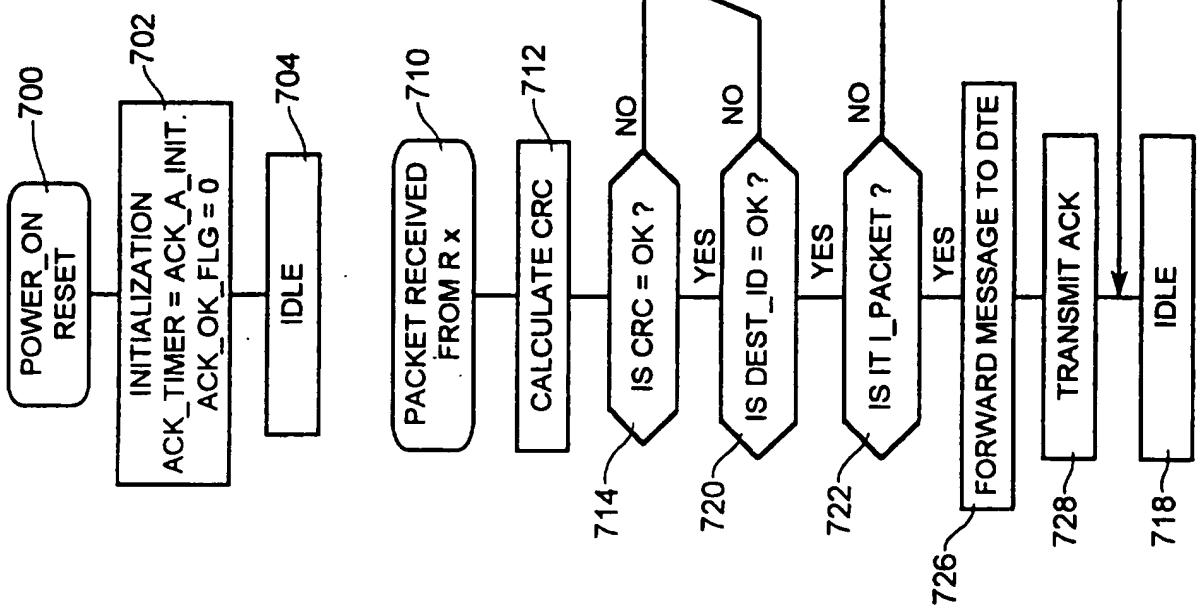

POWER_ON RESET
700
INITIALIZATION ACK_TIMER = ACK_A_INIT. ACK_OK_FLG = 0
702
IDLE
704
PACKET RECEIVED FROM R x
710
CALCULATE CRC
712
IS CRC = OK ?
714
NO
YES
IS DEST_ID = OK ?
720
NO
YES
IS IT I_PACKET ?
722
NO
YES
FORWARD MESSAGE TO DTE
726
TRANSMIT ACK
728
IDLE
718
ACK_TIMER = ACK_A_INIT. ACK_OK_FLG = 0
716
IS IT ACK_PACKET ?
724
NO
YES
ACK_OK_FLG = 1
725

FIG. 4

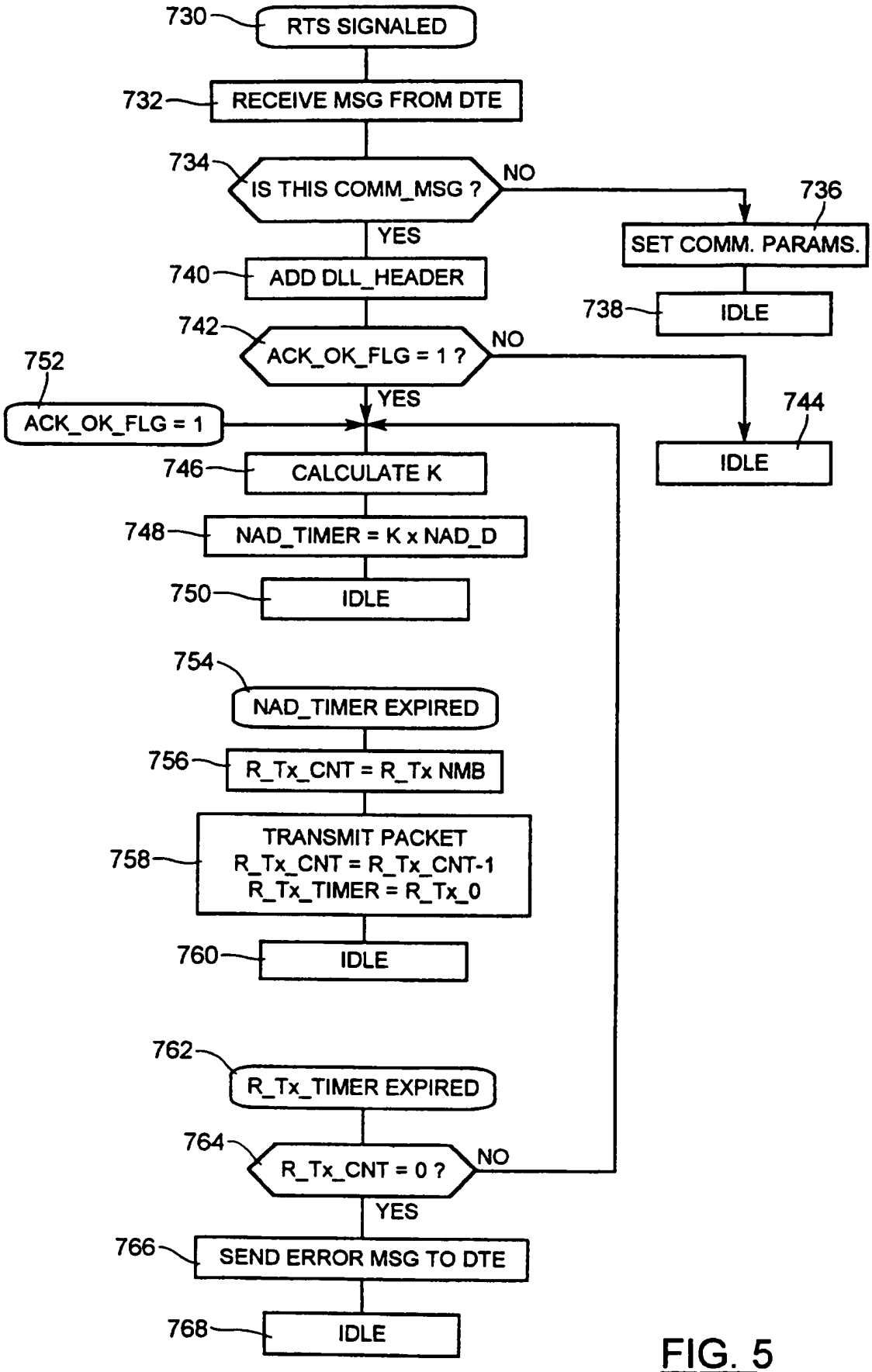

730
RTS SIGNALED
732
RECEIVE MSG FROM DTE
734
IS THIS COMM_MSG ?
NO
736
SET COMM. PARAMS.
YES
740
ADD DLL_HEADER
738
IDLE
742
ACK_OK_FLG = 1 ?
NO
752
ACK_OK_FLG = 1
YES
744
IDLE
746
CALCULATE K
748
NAD_TIMER = K x NAD_D
750
IDLE
754
NAD_TIMER EXPIRED
756
R_Tx_CNT = R_Tx NMB
758
TRANSMIT PACKET
R_Tx_CNT = R_Tx_CNT-1
R_Tx_TIMER = R_Tx_0
760
IDLE
762
R_Tx_TIMER EXPIRED
764
R_Tx_CNT = 0 ?
NO
YES
766
SEND ERROR MSG TO DTE
768
IDLE

FIG. 5

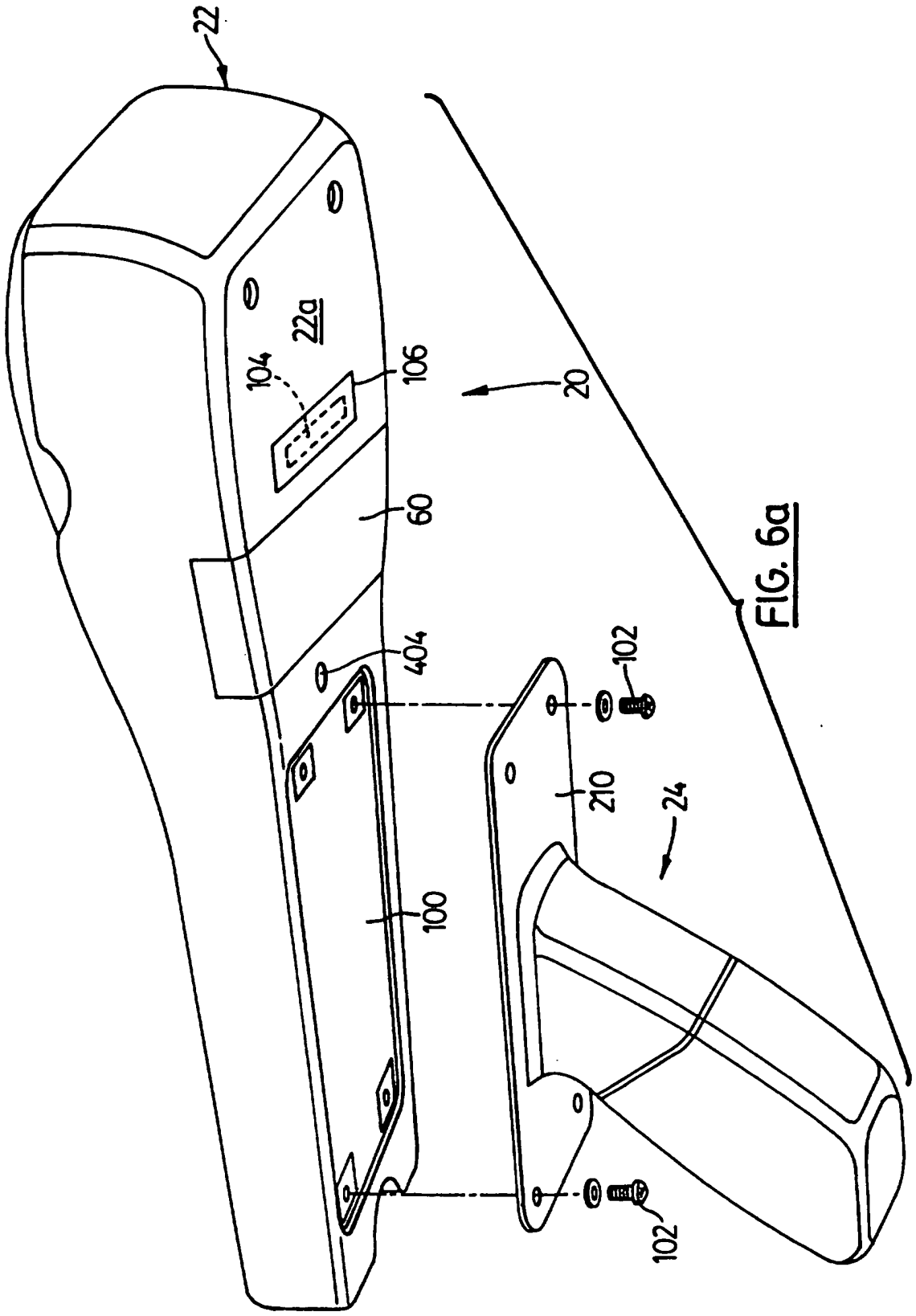


FIG. 6a

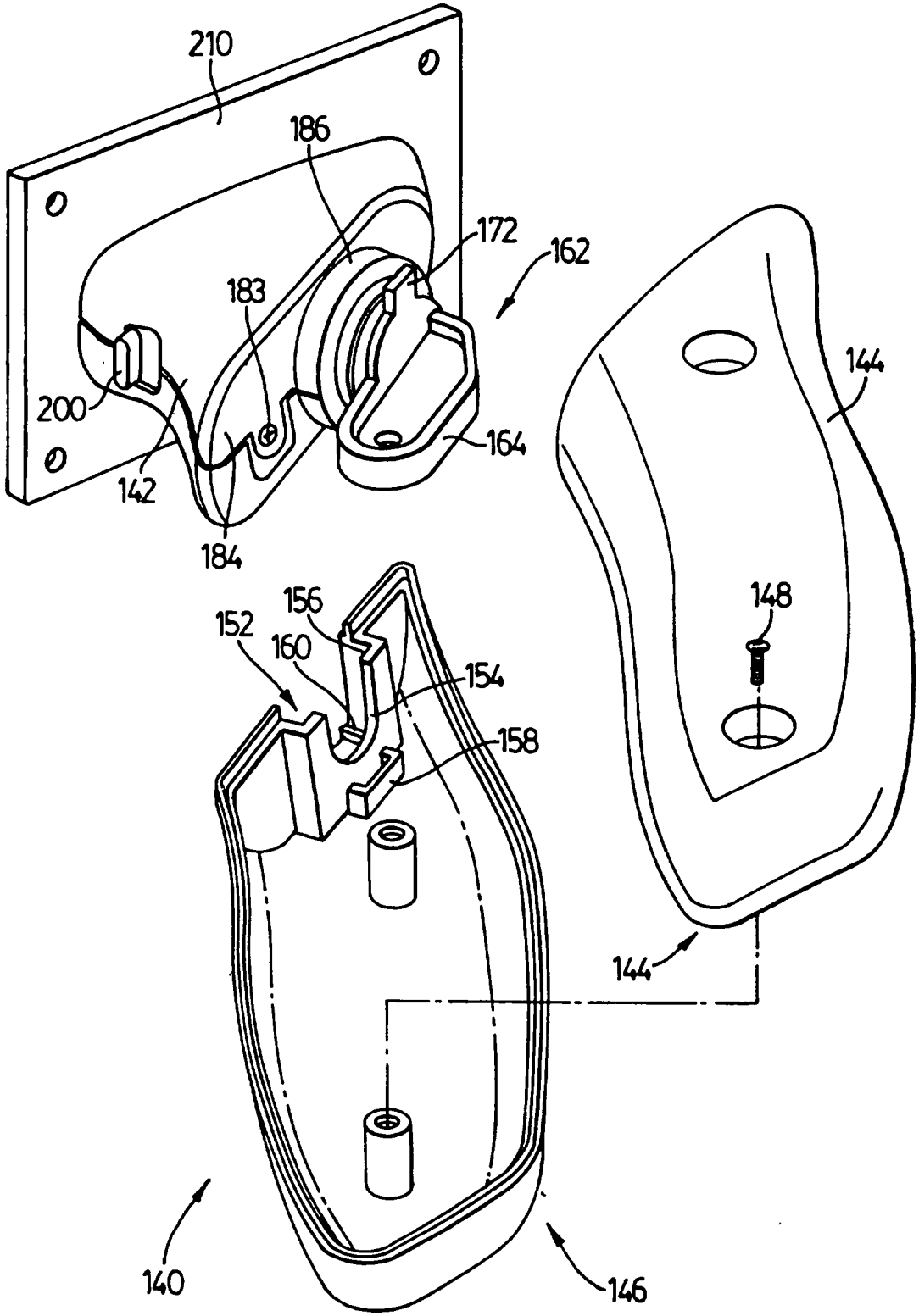

210
186
172
162
183
200
164
142
184
144
148
156
152
160
154
158
144
140
146

FIG. 6b

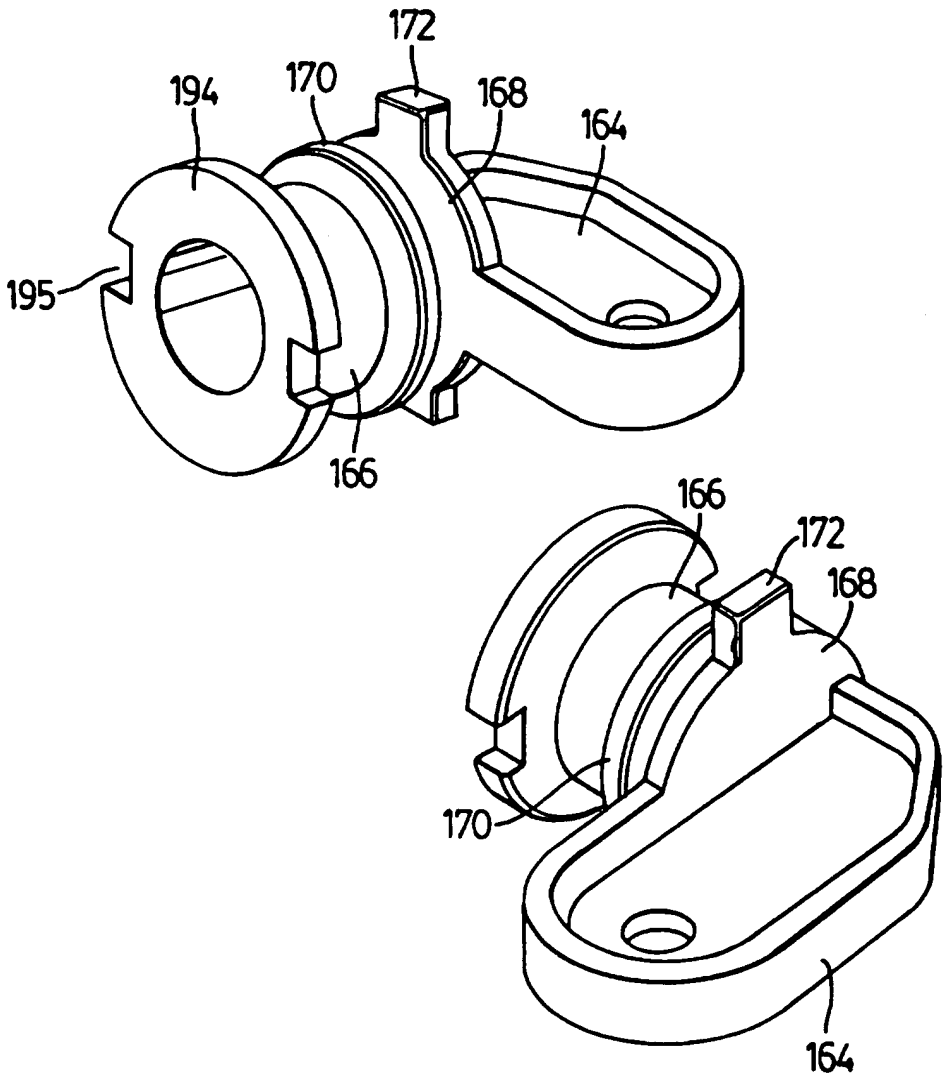

172
194
170
168
164
195
166
166
172
168
170
164
194
170
168
172
164
166

FIG. 6c

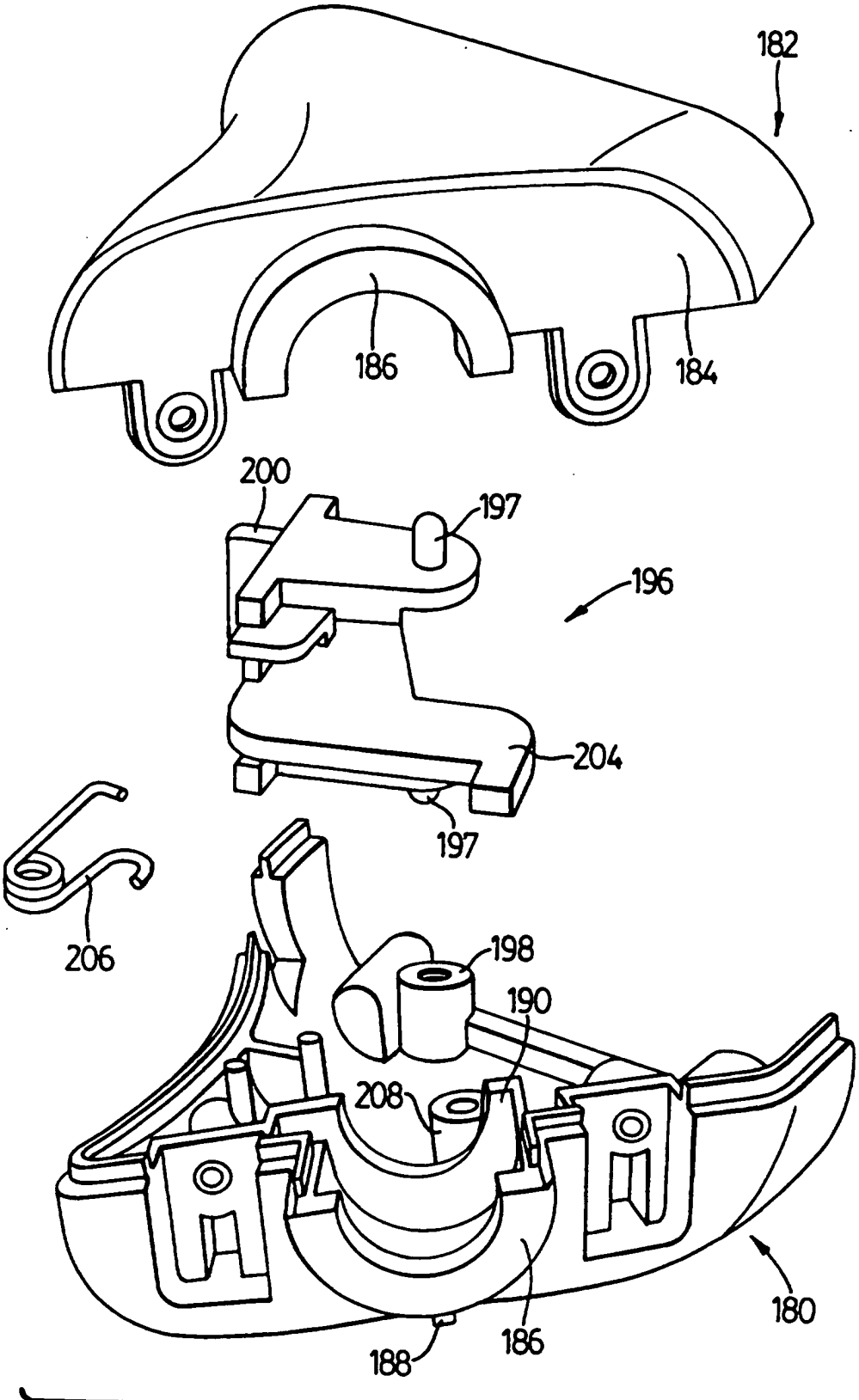


FIG. 6d

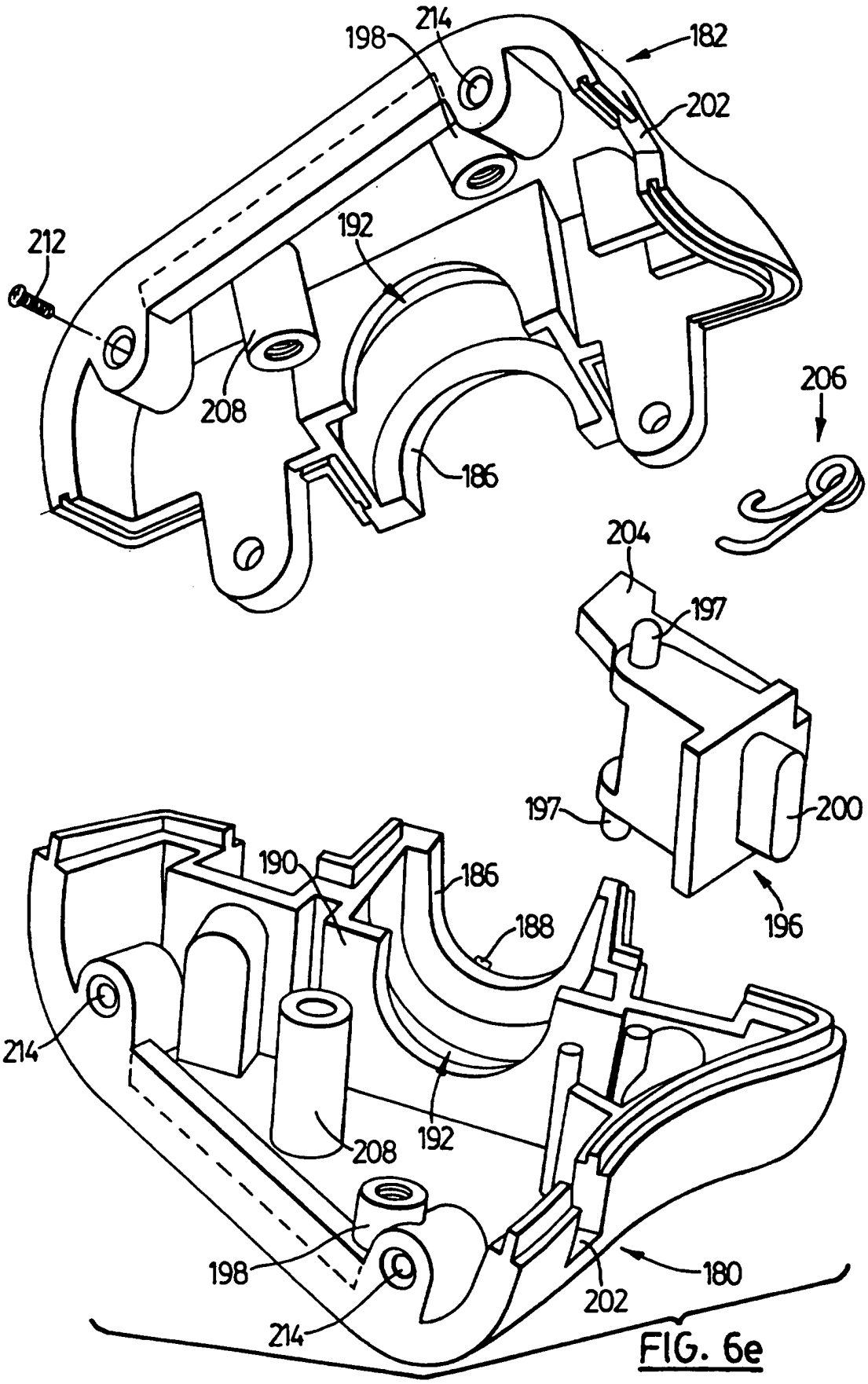

214
198
182
202
212
192
208
206
186
204
197
197
200
190
186
188
196
214
208
192
198
180
202
214

FIG. 6e

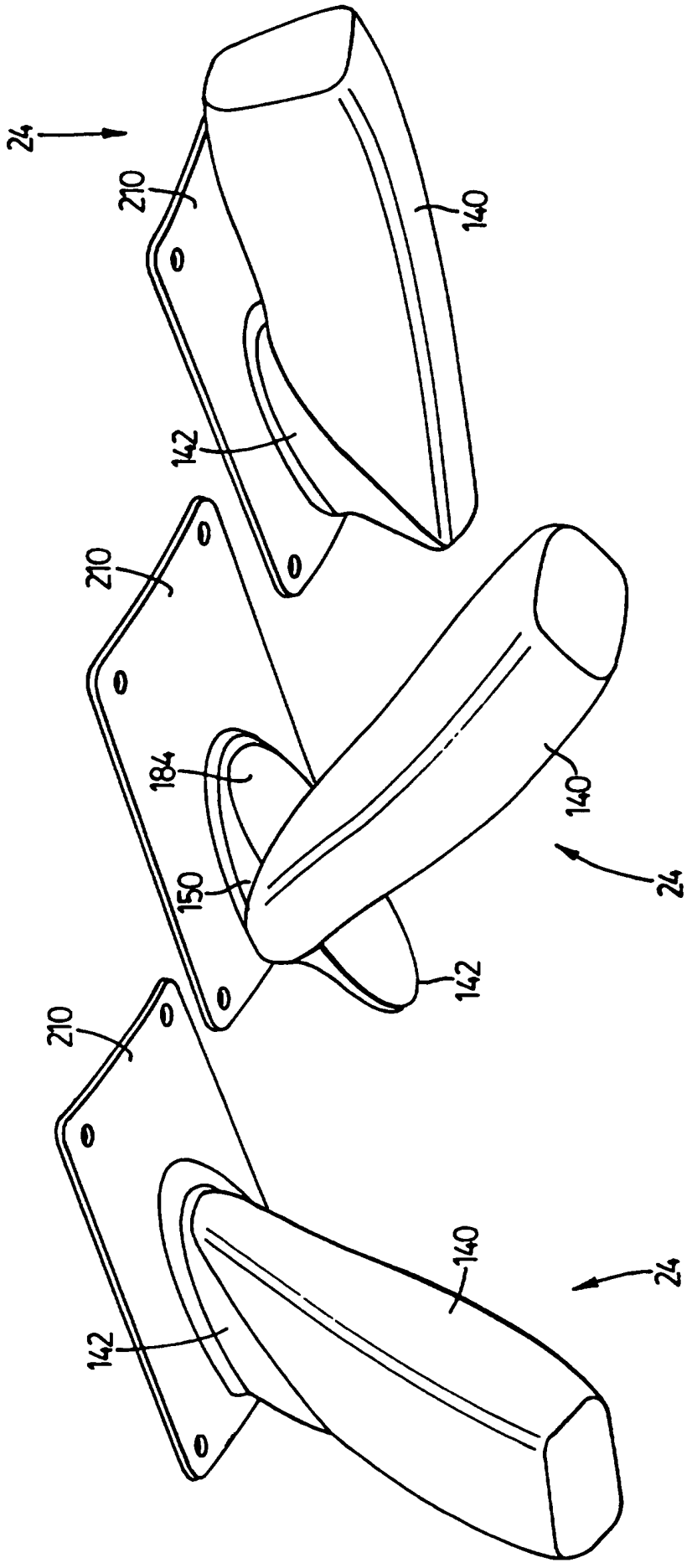


FIG. 7

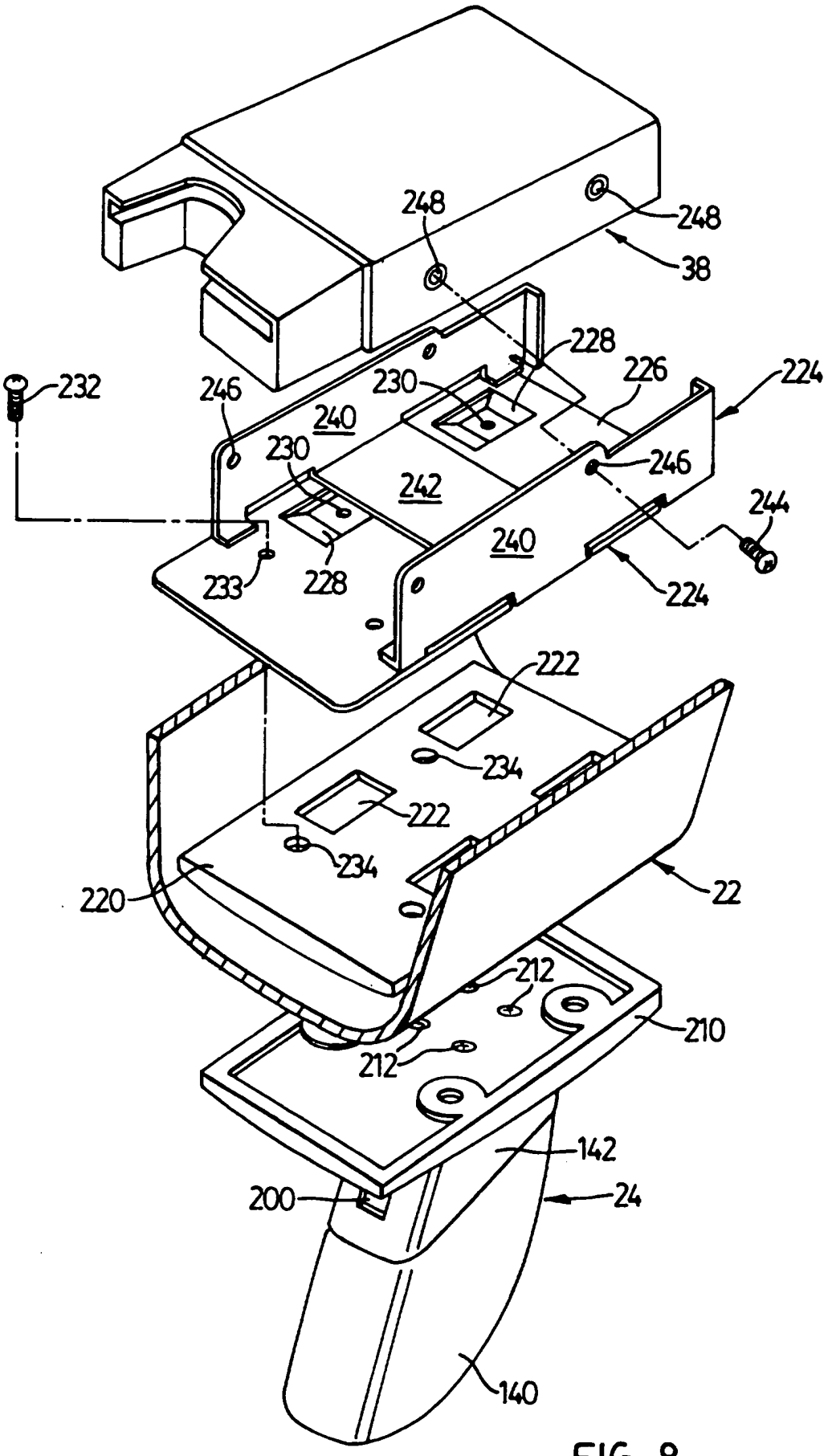

248
248
38
228
226
224
232
246
230
240
230
246
242
244
240
233
228
224
222
234
222
234
220
22
212
210
212
142
200
24
140

FIG. 8

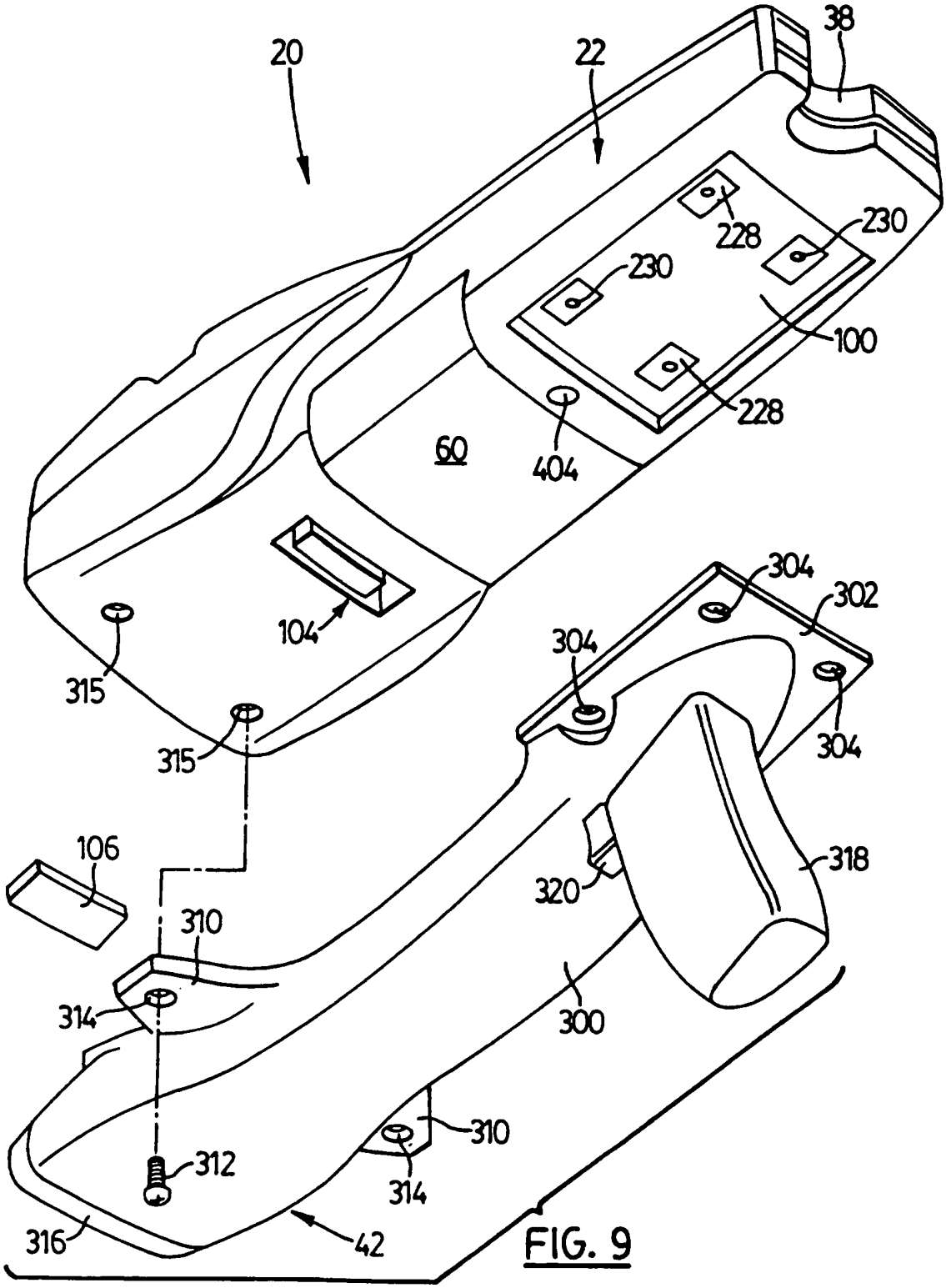

20
22
38
228
230
230
100
228
60
404
104
315
315
304
302
304
304
106
310
320
318
314
300
310
312
314
316
42

FIG. 9

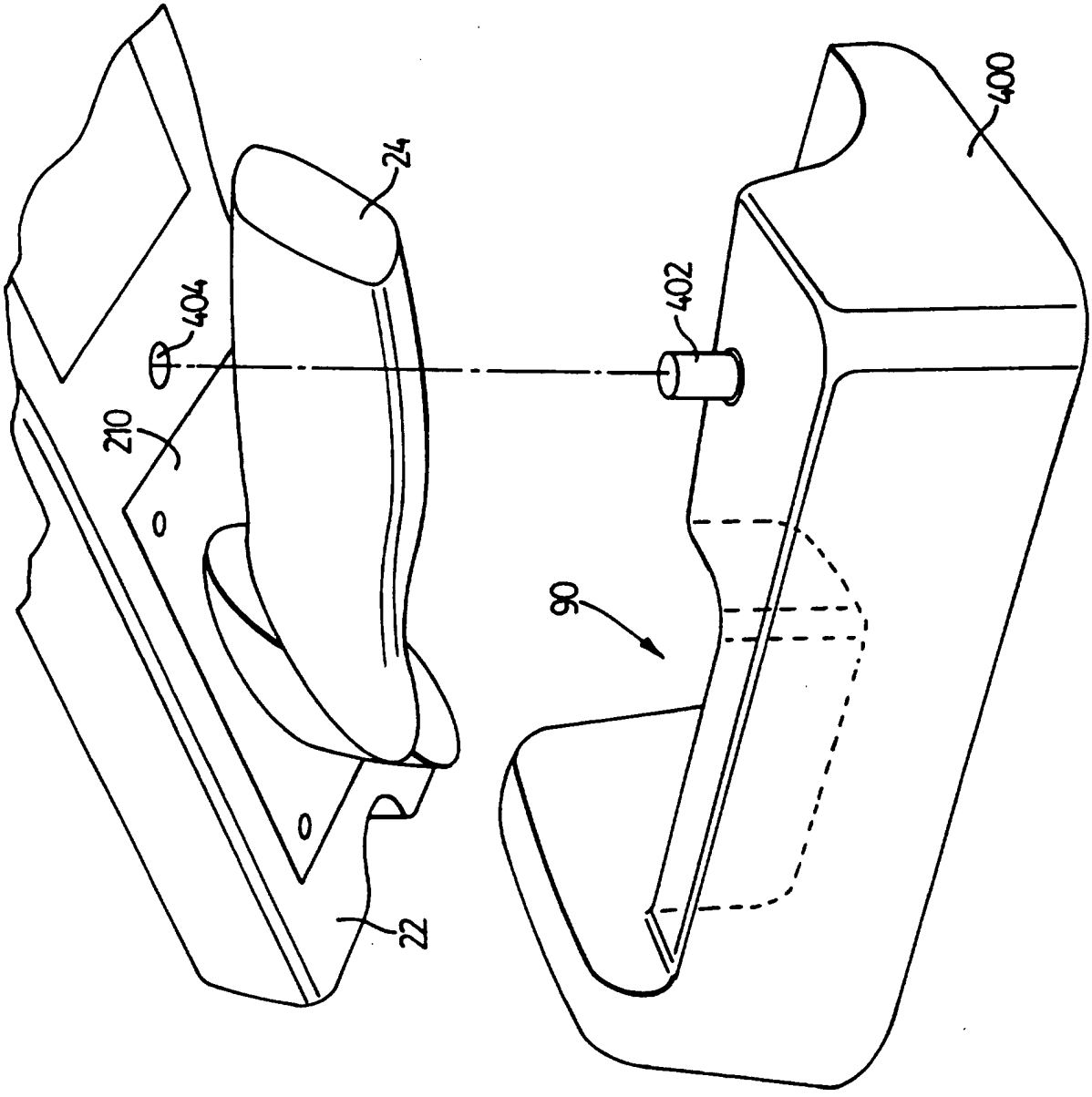


FIG. 10

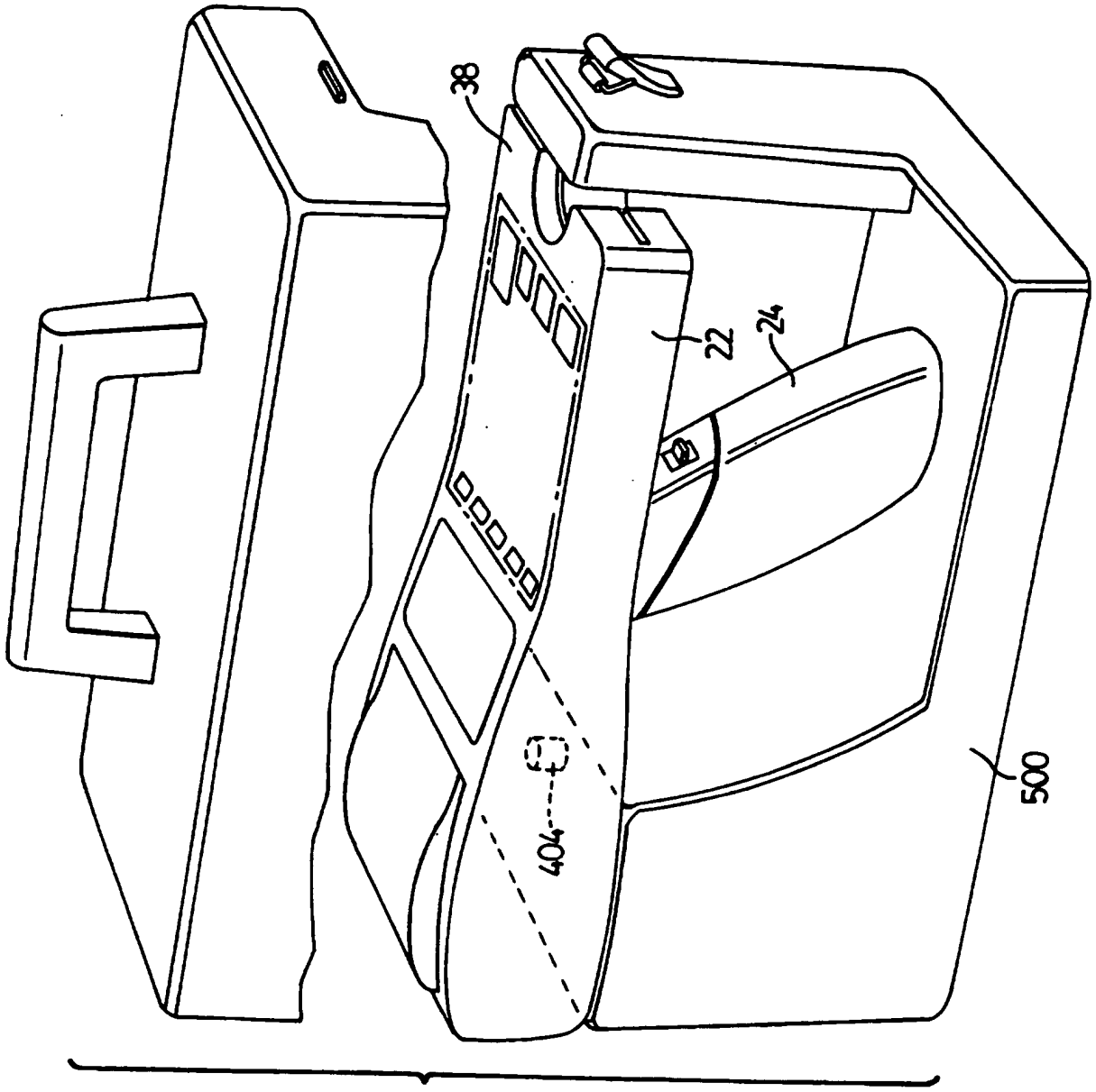


FIG. 11

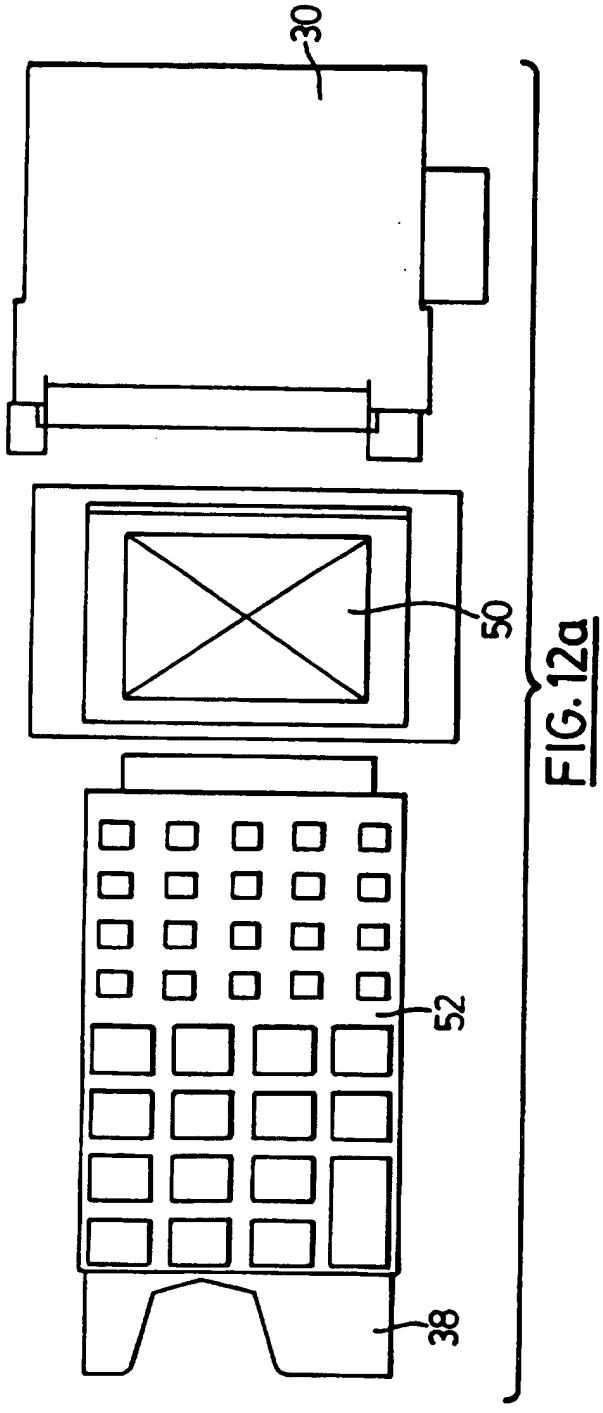


FIG. 12a

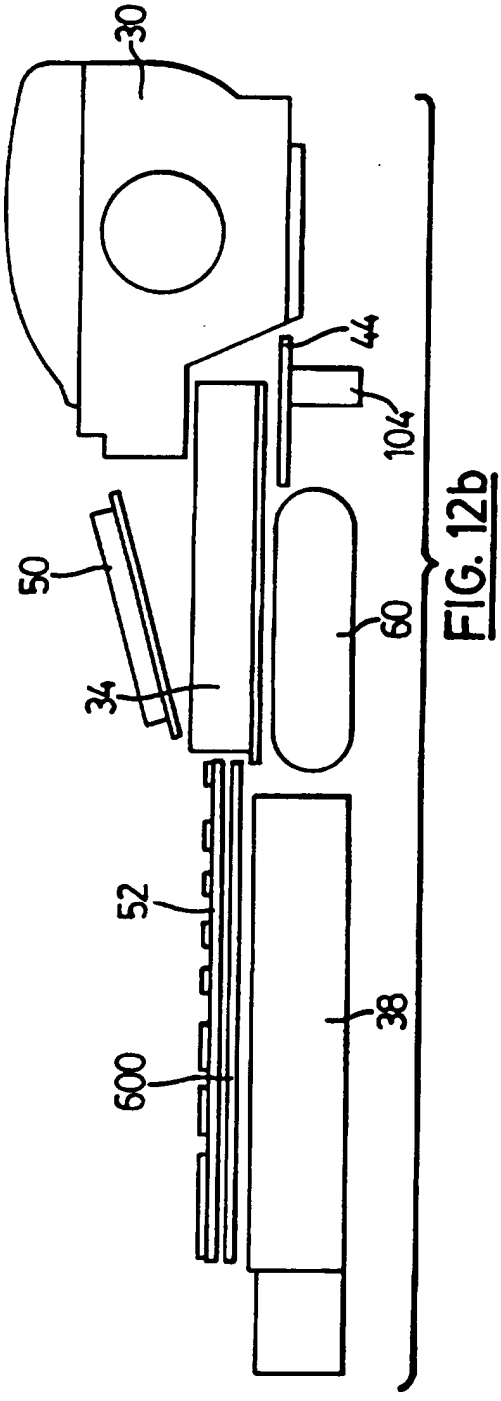


FIG. 12b

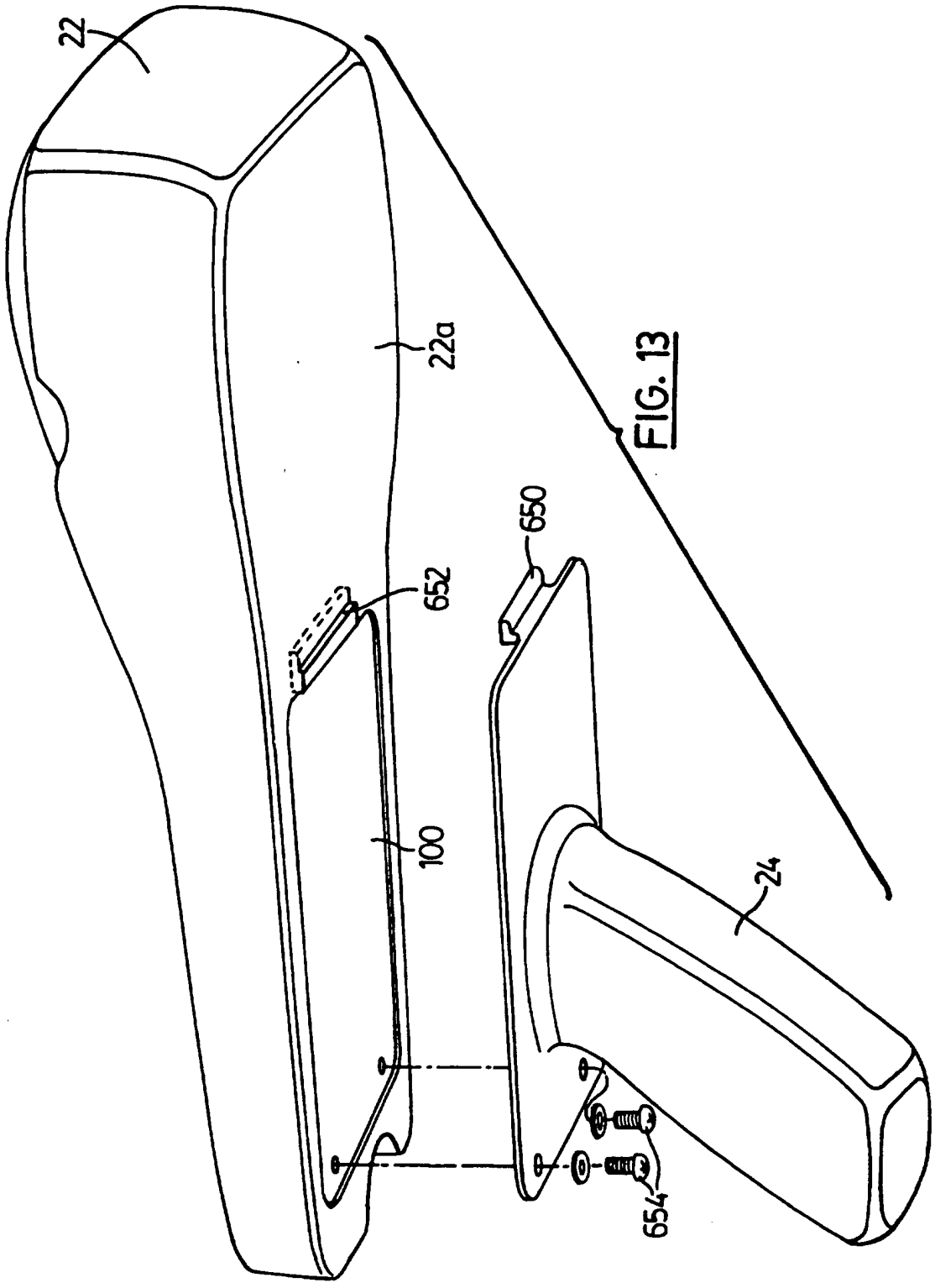


FIG. 13

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 96/00104

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US,A,5 208 446 (J.R. MARTINEZ) 4 May 1993	1-5,14, 15
A	see abstract; claims; figures see column 3, line 10 - line 55	17,19

X	EP,A,0 484 198 (SAGEM) 6 May 1992	1-3,5, 14,15
A	see the whole document	17,19

A	EP,A,0 456 548 (DASSAULT ELECTRONIQUE) 13 November 1991 see abstract; claims; figures	1,3-7,9, 14-17,19

A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 35, no. 1A, June 1992, NEW YORK US, pages 315-318, XP000308880 "PORTABLE SELF-CHECKOUT RETAIL SYSTEM" see the whole document	1,2,5,9, 12,14, 15,17,19

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 June 1996	27. 06. 96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer David, J

2

INTERNATIONAL SEARCH REPORT

:rnational Application No
PCT/CA 96/00104

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO,A,94 11849 (H. VATANEN) 26 May 1994 ---	
A	US,A,5 359 182 (D.I. SCHILLING) 25 October 1994 ---	
A	GB,A,2 151 061 (TICKETSHOP) 10 July 1985 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

'ernational Application No
PCT/CA 96/00104

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A-5208446	04-05-93	CA-A-	2091640	16-09-94
		GB-A,B	2276258	21-09-94
		US-A-	5334824	02-08-94
		DE-A-	4330254	30-06-94
		JP-A-	7093411	07-04-95
EP-A-0484198	06-05-92	FR-A-	2668629	30-04-92
		JP-A-	4264968	21-09-92
		US-A-	5387784	07-02-95
EP-A-0456548	13-11-91	FR-A-	2661998	15-11-91
		AT-T-	124157	15-07-95
		DE-D-	69110544	27-07-95
		DE-T-	69110544	07-03-96
WO-A-9411849	26-05-94	FI-A-	925135	12-05-94
		FI-A-	934995	12-05-94
		EP-A-	0669031	30-08-95
		NO-A-	951814	09-05-95
US-A-5359182	25-10-94	CA-A-	2107865	07-04-94
GB-A-2151061	10-07-85	NONE		